NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A RELIABILITY STUDY OF THE RFID TECHNOLOGY

by

Ng Ling Siew

December 2006

Thesis Advisor:	Tri T. Ha
Co-Advisor:	Weilian Su

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE A Reliability Study of the RFID Technology	5. FUNDING NUMBERS
6. AUTHOR(S) Ng Ling Siew	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT

RFID is a transformational technology that can bring about numerous benefits for its users. The US Department of Defense recognizes the potential benefits and has therefore issued a mandate for its suppliers to be RFID equipped. RFID allows for hands-free data capturing thus enabling the efficient recording of material transactions as well as increased efficiencies within the supply chain.

Accurate tag reads are vital for the successful implementation of an RFID system. The factors that affect the read reliability of an RFID system are examined in this paper. The extent to how these factors affect the reliability is studied and the possible methods of mitigating these factors are explored, with the aim of increasing the reliability of reading single tags. Specific study into alternative coding and modulation techniques is done, and their performance compared with techniques used in the existing technology.

14. SUBJECT TERMS Radio frequency identification (RFID) systems, reliability, passive tags, coding techniques, modulation techniques	15. NUMBER OF PAGES 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

A RELIABILITY STUDY OF THE RFID TECHNOLOGY

Ng Ling Siew
Design Engineer, Singapore Technologies Marine Ltd
B.Eng., National University of Singapore, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Author: Ng Ling Siew

Approved by: Professor Tri T. Ha
Thesis Advisor

Professor Weilian Su
Co-Advisor

Professor Jeffrey B. Knorr
Chairman, Electrical and Computer Engineering Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

RFID is a transformational technology that can bring about numerous benefits for its users. The US Department of Defense recognizes the potential benefits and has therefore issued a mandate for its suppliers to be RFID equipped. RFID allows for hands-free data capturing thus enabling the efficient recording of material transactions as well as increased efficiencies within the supply chain.

Accurate tag reads are vital for the successful implementation of an RFID system. The factors that affect the read reliability of an RFID system are examined in this paper. The extent to how these factors affect the reliability is studied and the possible methods of mitigating these factors are explored, with the aim of increasing the reliability of reading single tags. Specific study into alternative coding and modulation techniques is done, and their performance compared with techniques used in the existing technology.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author acknowledges the support of many people in making this research possible.

She would like to express her sincere thanks to Prof Tri Ha for his guidance and support in this work, and for sharing his wealth of knowledge in the area of digital communications. His ideas and criticisms have helped much in improving the quality of this work.

She is also grateful to Prof Weilian Su for his professional advice and invaluable insights that has helped in the refinement of this work.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Improving the read reliability of individual Radio Frequency Identification (RFID) tags is important to the military's goal of achieving a supply chain management system with item level tagging. Item level tagging improves the ability of suppliers to plan, meet demands and streamline business processes. The benefits to the military are a better inventory management, better productivity and improved asset tracking.

The goal of a supply chain management system with item level tagging, was first demonstrated by Walmart, when she mandated her top 100 suppliers to be RFID ready by 2005. The DoD also issued a similar mandate, and committed to the implementation item-level tagging with RFID technology, with additional funding and the issue of policies to suppliers.

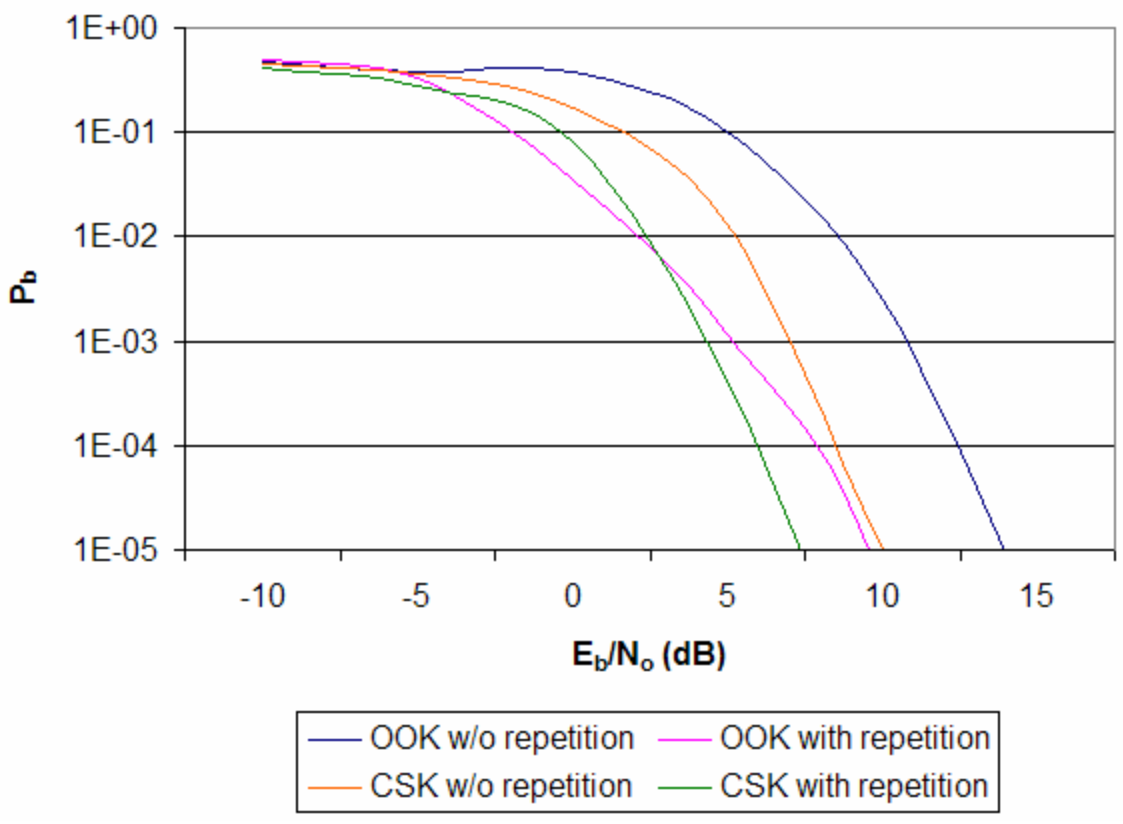
Due to the limitations of the current RFID technology, Walmart and the DoD have only been able to implement pallet level tagging. 100% read reliability for pallet level tagging has not been achieved, and hence, item level tagging, which requires multiple tags to be read simultaneously, is not yet achievable.

Accurate tag reads are vital for the successful implementation of a RFID system. The objective of this study is to improve the read reliability of RFID systems. This study looks at the current RFID technology, focusing on the problems and limitations of the technology, when deployed in a single tag to single reader environment. Several factors may affect the read reliability of an RFID system. They include speed, distance, orientation, coding techniques, power, sensitivity and error detection. Many of these factors result in signal attenuation, which reduces the signal-to-noise ratio (SNR). Simulink models are used to study the effects of the factors listed above. The simulation runs shall examine the variation of the bit error probabilities as SNR changes.

Data is typically coded using on-off keying (OOK) in the existing RFID systems. Our simulations revealed that with OOK, an SNR of 12.5 dB is required

to achieve a bit error rate of 10^{-4}. Often, due to environment conditions, orientation of tags, and other uncontrollable factors, this SNR is not attainable.

This research explores alternative coding techniques with the aim of finding techniques that yield better bit error rate performance, looking at repetition coding, code shift keying, and a combination of the two. With repetition coding, performance is improved by approximately 4 dB when each bit is repeated five times, resulting in a SNR of 8.5 dB for a bit error rate of 10^{-4}. The use of code shift keying (CSK) requires a SNR of 8.5 dB to achieve the same bit error rate performance of 10^{-4}. The final method of coding, which involves the repetition of each bit before CSK, achieves a 2.5 dB improvement over the previous methods, requiring a SNR of 6 dB. This is a coding gain of 6.5 dB as compared to OOK.



Comparison of BER performance

This research examines the building block of the item-level tagging goal of Walmart and DoD, improving the individual read reliability of a single tag in a single reader environment. The use of CSK with repetition coding reveals a lower requirement for SNR, achieving a better read reliability, thereby making the RFID system more reliable.

This research focuses on the single tag problem. Future work can explore the impact of having multiple tags in the interrogation zone. Analysis on whether the codes provide any advantage in terms of resolving collisions can also be explored. In addition, enhancements to the model to take into account other factors such as reflections by objects in the vicinity could be made. The effect of such reflections on read reliability can be studied.

Given the vast potential that this transformational technology has on numerous industries other than Walmart and DoD, it is imperative that continued research on improving the read reliability of RFID systems be conducted.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Walmart's announcement of requiring its top 100 suppliers to be Radio Frequency Identification (RFID) ready by 2005, sparked off the recent interest in RFID technology. Walmart aims to improve its supply chain management system by item-level tagging. With similar goals, the US Department of Defense (DoD) has also issued a similar mandate to its suppliers. Since then, the current RFID technology only allows for pallet level tagging, where 100% read reliability has not been achievable. Item level tagging requires multiple tags to be read simultaneously, and this poses a much more complicated problem.

This research examines the current RFID technology, when deployed in a single tag to single reader environment. The factors affecting the read reliability of RFID systems will be studied. These factors include speed, distance, attenuation, orientation, coding techniques, power, sensitivity, and error detection. The extent to which these factors affect the reliability will be examined, and possible methods of mitigating these factors will be explored, with the aim of the increasing the reliability of reading single tags.

A. DEFINITION OF RELIABILITY

The standard military definition of reliability is "the probability that an item will perform a required function without failure under stated conditions for a stated period of time." (US DoD, Military Handbook 217).

Reliability also refers to the probability that a component or system will operate satisfactorily, either at any particular instant when it is required, or for a certain length of time (Wolstenholme, 1999).

This research focuses on an individual tag's read reliability. For a RFID system, in a particular operating environment, tag readability can be defined as the capability of the system to read a specific tag data successfully (Lahiri, 2006).

The definition adopted by this research for tag reliability refers to the probability that a tag will be read correctly for a particular operating environment.

For a tag containing *n* bits of data, where each bit has a probability of bit error of P_B, the tag can only be read successfully if all the bits are correctly read. Thus, the probability that a tag will be read correctly is given by the following equation:

$$P_{success} = (1 - P_B)^n$$

B. RFID SYSTEM OVERVIEW

The RFID technology allows the identification of objects using radio waves. With the use of radio waves, the major advantage is that line-of-sight access (LoS) is not necessary. However, the use of radio waves presents several challenges for the technology. These challenges include distance constraints, power constraints, and environmental constraints.

An RFID system consists of two main components: the tag and the reader. The tag is typically embedded in the object of interest, and the reader is the device that identifies the object through the use of radio waves.

1. RFID Tag

A RFID tag stores and transmits data to the reader, and can be either passive or active devices. Passive RFID tags draw their operating power from the electrical field generated by the RFID reader, thus requiring the reader to be in close proximity. Active tags are self powered (by an internal battery), thus achieving a greater read range. The choice of RFID tags depends largely on the application that it will be installed.

2. RFID Reader

A RFID reader (commonly known as an interrogator) reads information from RFID tags. Each reader is made up of a transmitter and receiver, where the transmitter transmits radio signal into the environment, and the reader receives the transmitted signals and sends it to a microprocessor for processing.

Readers have antennas that are physically attached by way of a cable. The position of the antenna affects the antenna's characteristics, thereby affecting read reliability.

The theoretical antenna pattern is an ellipsoid. However, antenna patterns are not always uniformly shaped in real life. Protrusions and nulls within the pattern are common and unpredictable, resulting in dead zones, where readability can be significantly affected (Lahiri, 2006).

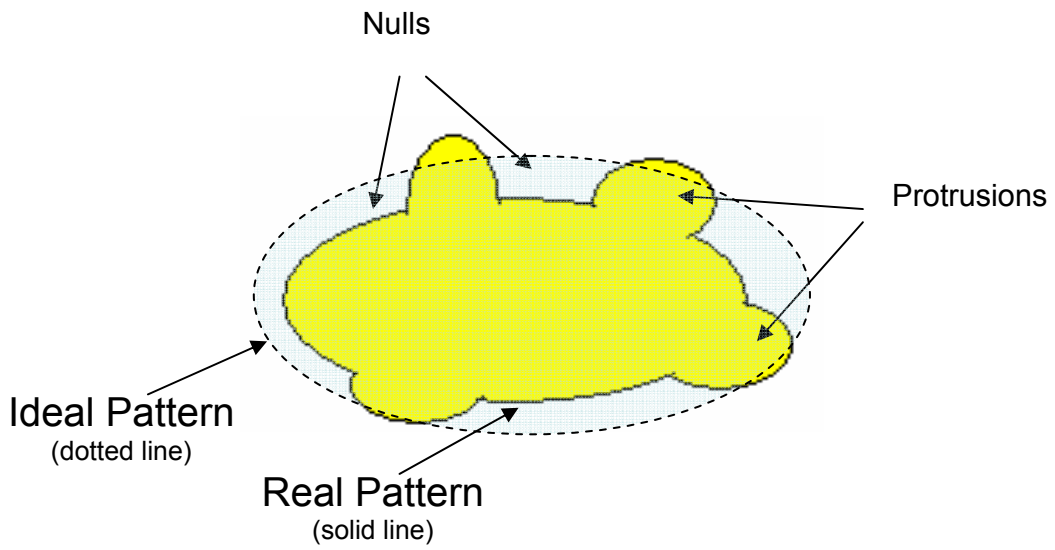


Figure 1. An ideal vs a real antenna pattern.

Readers can be fixed or mobile. Fixed readers are mounted on structures such as a wall, or inside a delivery truck, and typically use external antennas. Mobile units are usually handheld, and they generally use built-in antennas.

C. OPERATING FREQUENCIES

The choice of operating frequency is the key for an RFID system as the maximum read range (distance between the tag and the reader) achievable is largely dependent on the operating frequency. The operating frequencies for RFID systems range from low frequencies (LF) and high frequencies (HF) to ultra-high frequencies (UHF) and microwave frequencies (MW).

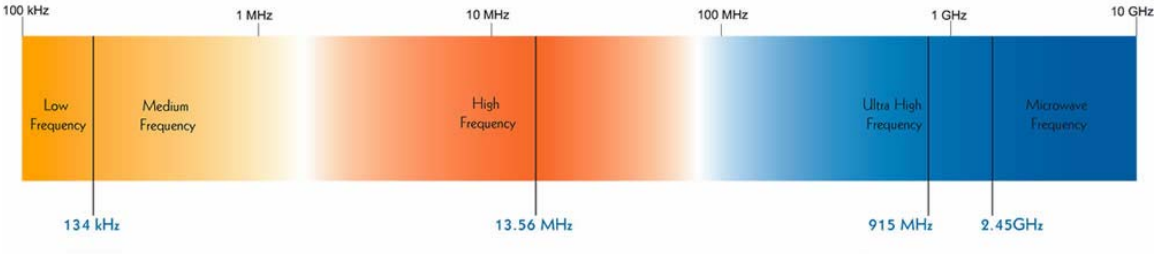


Figure 2. RFID Frequency Spectrum Table (from Electro-com).

Near field communication is used for RFID systems operating in the LF and HF range, whilst far field communications is used when the RFID operates in the UHF and MW as shown in the figure below.

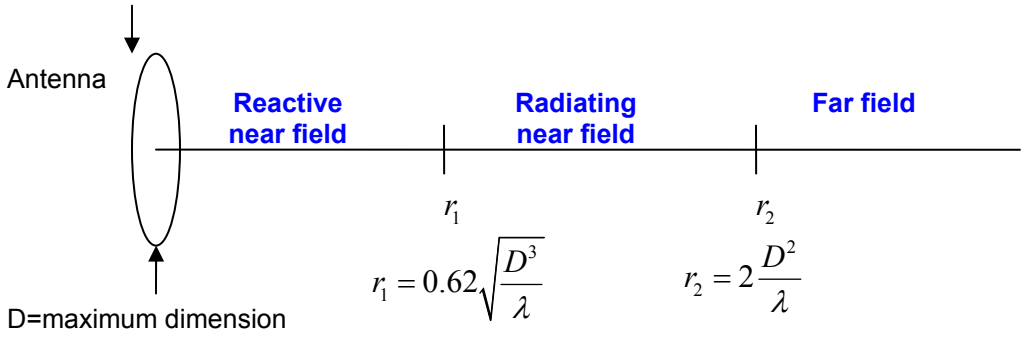


Figure 3. Field regions.

Signal strength in near field communications is attenuated by the cube of the distance between the reader and antenna, while that for far field is attenuated by the square of the distance between the two (Lahiri, 2006). As such, the read range is longer with the UHF and MW (see table 1).

The application in which the RFID system is deployed determines the choice of operating frequencies. Short-range applications such as livestock identification and electronic door locking systems use LF. Small product labeling typically use HF. Highway toll-collection applications (such as the Electronic Road Pricing System in Singapore) typically uses UHF. The typical maximum read range for passive tags are listed in the table below (Glover & Bhatt, 2006).

Frequency Band	Maximum Range (meters)
LF	0.5 meters
HF	3 meters
UHF	9 meters
MW	>10 meters

Table 1. Typical maximum read ranges.

Each frequency band has definite advantages and disadvantages. The advantages and disadvantages are summarized in the following table:

Operating Frequency	Advantages	Disadvantages
Lower frequencies	Low operating power Inexpensive Not sensitive to orientation Can be read thru metallic overlays	Short read distances Slower data rate Noise sensitive
Higher frequencies	Greater read distances Higher data transmission rate Less sensitive to noise	Higher operating power More expensive Orientation sensitive Cannot be read thru metallic overlays

Table 2. Frequency attributes (adapted from Shepard, 2005).

Depending on the application in which the RFID system is to be deployed, suitable operating frequencies need to be chosen. Low frequency tags use less

power and are better able to penetrate metallic objects. They have short read ranges and are sensitive to noise. These properties make them suitable for access control systems, and for hazardous waste monitoring. Higher frequencies however require higher operating power. This means that a separate source of power (like an onboard battery) might be needed to provide sufficient power. In addition, they are able to achieve higher read range and higher data transfer rates. As such, higher frequencies are suitable for road toll systems and baggage handling.

D. COMMUNICATION PROTOCOL

Communication between tags and readers can take on one of the following forms: modulated backscatter, transmitter type or transponder type.

1. Modulated Backscatter

In the modulated backscatter mode of communication, readers send out an RF signal containing AC power and a clock signal. The tags draw power from the readers and are thus energized to perform either read or write functions.

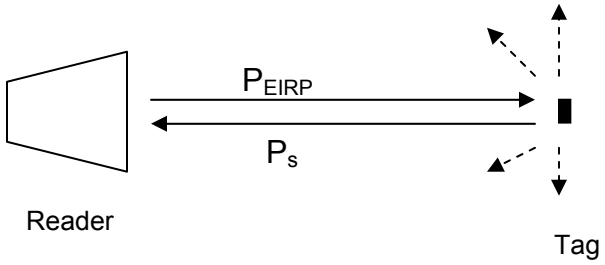


Figure 4. Backscatter – Reflection of electromagnetic waves

The radiation density S that reaches the tag at distance r away from the reader is given by (Stutzman & Thiele, 1997):

$$S = \frac{P_{EIRP}}{4\pi r^2}$$

The tag reflects a power P_s that is proportional to the power density S and the radar cross-section σ:

$$P_s = S \times \sigma$$

This reflected power travels through space, and back to the reader. The power decreases in proportion to the square of the distance r^2; the radiation density that reaches the reader is given by:

$$S_{back} = \frac{P_s}{4\pi r^2}$$

The radar cross-section σ is a measure of how well an object reflects electromagnetic waves. It depends on a large array of parameters including surface area of object, shape of object, material, and the surface structure of object. Due to the numerous factors that can affect the radar cross-section σ, it is difficult to obtain a precise value for σ. To compound the problem, objects of differing properties exists in the RFID system's operating environment. The electromagnetic wave emitted into space is scattered in many directions with varying intensities. Waves that hit radar absorbing materials (such as plastics) are absorbed, while those that hit metal surfaces are reflected. The reflected waves from the objects can add constructively or destructively. Hence, simulations cannot properly take into account the electromagnetic reflections. To find the actual power reflected back to the reader, a physical experiment needs to be conducted.

Tags utilizing this scheme can only communicate in the presence of a reader as it relies on the reader's power to transmit data.

2. Transmitter Type

The transmitter type applies only to active tags. Tags broadcast their data at regular intervals. Readers that are in range are able to receive the data when required.

3. Transponder Type

With the transponder type, tags only send data to readers upon request. Tags utilizing this mode of communication enter a 'sleep' state when no request for transmission is made. Periodically, the tag sends a message to check if any

reader is waiting for transmission. Readers that receive this message can instruct the tag to ‘wake up’ and begin transmission.

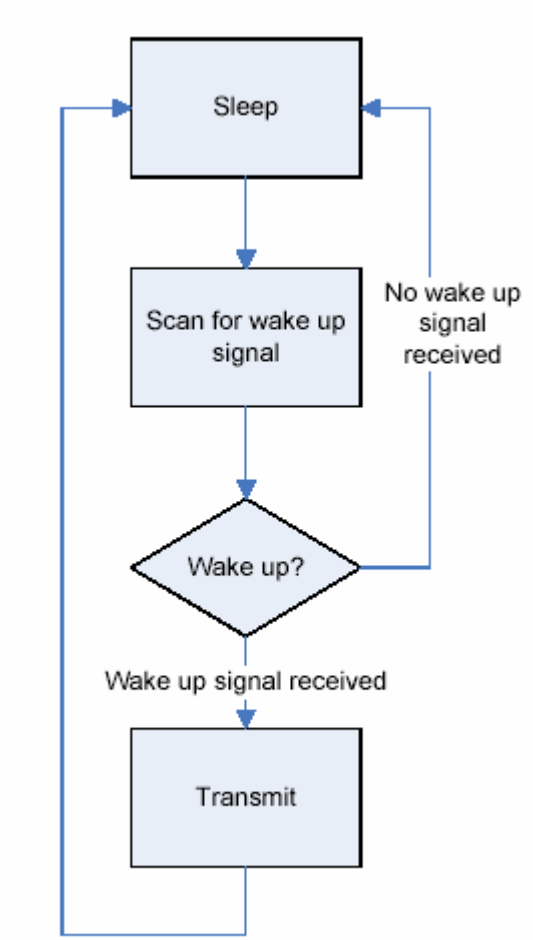


Figure 5. Transponder type communication protocol for a typical RFID tag.

E. MOTIVATION FOR RESEARCH

The individual building blocks that form the RFID technology are simple. The amalgamation of these blocks forms a technology that has vast potential. A definite niche exists for this advanced technology.

To achieve the goal of item-level tagging, there is a strong need to achieve better read reliability of individual tags which currently stands at about 80%. Once the reliability of a single tag is achieved, future studies can then delve into improving the reliability of reading multiple tags.

F. RESEARCH OBJECTIVES

This research seeks to identify the factors that affect the read reliability of RFID tags, and determine the extent of how these factors affect the read reliability. Possible methods of mitigating these factors are explored, with the aim of increasing the reliability of reading single tags. Specific study into alternative coding and modulation techniques are conducted, and their performance compared with techniques used in the existing technology.

G. ORGANIZATION OF THESIS

This chapter is written with the aim of giving the reader a brief overview of an RFID system, as well as to put forth the definition of reliability that is used as the measure of performance in our study. The rest of the thesis is organized as such:

Chapter II examines the current technology, identifying the factors that affect the reliability of the RFID system.

Chapter III analyses the current technology, and details the methodology, and simulation model used for this research.

Chapter IV proposes alternatives for improved performance. Performance analysis of the proposals will be carried out, with results presented in this chapter as well.

Chapter V reviews the U.S. Department of Defense (DoD) RFID policy and highlights how proposed alternatives meet the current DoD requirements.

Recommendations for future work and conclusions of our study will be presented in Chapters VI and VII.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FACTORS AFFECTING READ RELIABILITY OF RFID SYSTEMS

Read reliability of RFID systems are affected by several factors. The presence of these limiting factors prevents the technology from achieving its maximum potential. These factors include distance, environment, orientation, encoding techniques, and power. The effects of these factors will be examined, and possible methods of mitigating these factors will be explored, with the aim of increasing the reliability of reading single tags.

A. DISTANCE

The RF beam is typically in the shape of an ellipsoid – the beam becomes wider as the distance from the source increases. This poses challenges in terms of distance (between the reader and the tag).

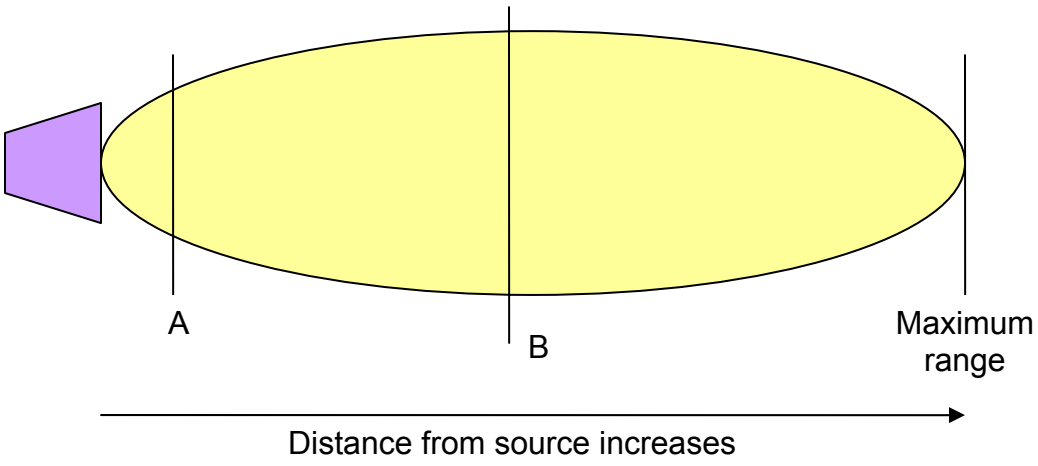


Figure 6. Range of coverage.

The number of tags that can be within the read range at point B is significantly greater than that at point A. Hence, as the distance from the source increases, the possibility of having more than one tag within the interrogator's zone increases. Tag collision might occur as a result.

In addition, the signal strength in near field communications is attenuated by the cube of the distance between the reader and antenna, while that for far field is attenuated by the square of the distance between the two (Lahiri, 2006). As such, we can expect the degradation due to distance to follow either a cubic or squared decline to some extent.

The maximum read range of a reader can be controlled by power and sensitivity settings. The optimal power and sensitivity settings can be chosen based on the application in which the RFID system is deployed.

B. POWER

Power is supplied to the tags through electromagnetic backscatter coupling. A continuous carrier wave with AC power is transmitted by the reader's antenna. The tag uses this power to modulate the received signal, encoding its data, and subsequently transmitting it back to the reader.

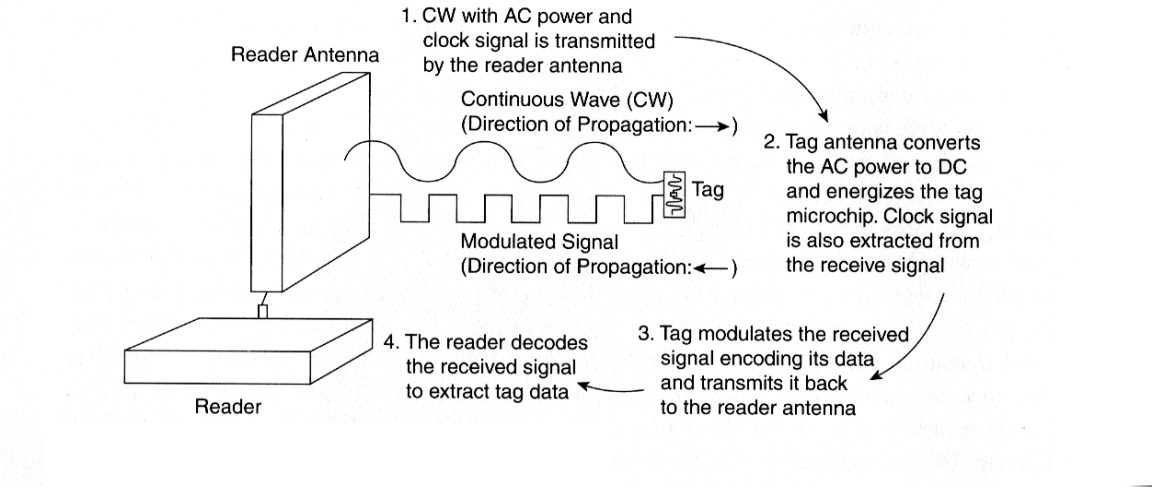


Figure 7. Electromagnetic backscatter (from Lahiri, 2006).

As the transmitted signal traverses the atmosphere, its power level decreases. If the power level drops below a certain threshold (determined by the sensitivity of the reader), the reader may not be able to accurately receive the data.

The maximum peak output power of an intentional radiator is regulated by the Federal Communications Commission (FCC) in the United States. The allowable power level varies for systems operating in different frequency bands, with the highest allowable power being 1 Watt (FCC, 2006).

In backscatter communication system, Signal-to-Noise Ratio (SNR) must meet a required threshold. A solution to achieving an acceptable SNR is to increase the transmission power (Cha, 2006). However, this increase has to be within FCC acceptable level.

C. ENVIRONMENT

The presence of metals, liquids and objects that absorb or reflect RF waves might affect the read accuracy of tags. Multipath fading occurs when the antenna signals are reflected off an object. The presence of wireless networks, or electronic devices such as motors and motor controllers, also interferes with the RFID readers. Noise emitted from such devices prevents readers from an accurate read.

The presence of RF opaque and RF absorbent materials effectively prevents the waves from traveling from the antennas to the readers. RFID readers do not perform well when tags are embedded within RF opaque or RF absorbent materials. The reader may fail partially or even completely. This limitation is particularly apparent when UHF or MW is used. When the reader tries to read a tag contained within an RF opaque material such as a metal enclosure or some RF absorbent material like water or rain, its performance is significantly degraded. The presence of human traffic within an operating environment also affects the performance of RFID readers as humans act as dampeners, attenuating the signals from the antennas.

D. ORIENTATION

Orientation refers to the position of the tag in relation to the reader. Tags that are insensitive to orientation are able to work regardless of its orientation. RFID systems operating at higher frequencies are more sensitive to orientation, performing well at certain angles, and degrade at certain angles, sometimes to a point (null zone) where it cannot be read at all. Orientation sensitivity is most apparent when a linear polarized antenna is used. A linearly polarized dipole antenna transmits and receives best when the tags are parallel to its axis. When the tag reader and antenna reader are aligned, the maximum read distance can be achieved. If the tag and reader antennas are misaligned, only a small portion of the energy emitted by the reader will hit the tag antenna, causing readability issues. The figure below illustrates this. Tag antennas are typically mounted flat in the plane of the tag. If the tag is aligned parallel to the polarization direction of the reader antenna, good readability can be achieved.

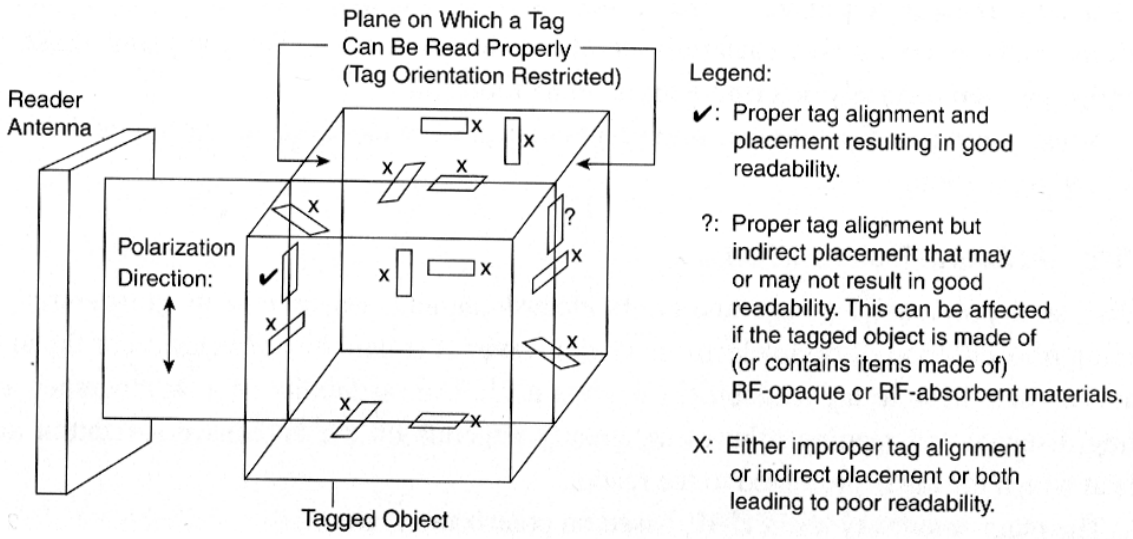


Figure 8. Proper Orientation of Tags for Linearly Polarized Antennas (from Lahiri, 2006).

E. ENCODING

Data embedded within RFID tags consists of n bits of data, with each bit either a binary 1 or 0. Some of the frequently used encoding for the transmission of binary data includes Unipolar, NRZ, Unipolar RZ, Bipolar and Manchester coding. Presently, the data stored in RFID tags are typically coded using Unipolar (also commonly known as on-off keying), polar, Unipolar return-to-zero, or Manchester coding (as shown in the figure below).

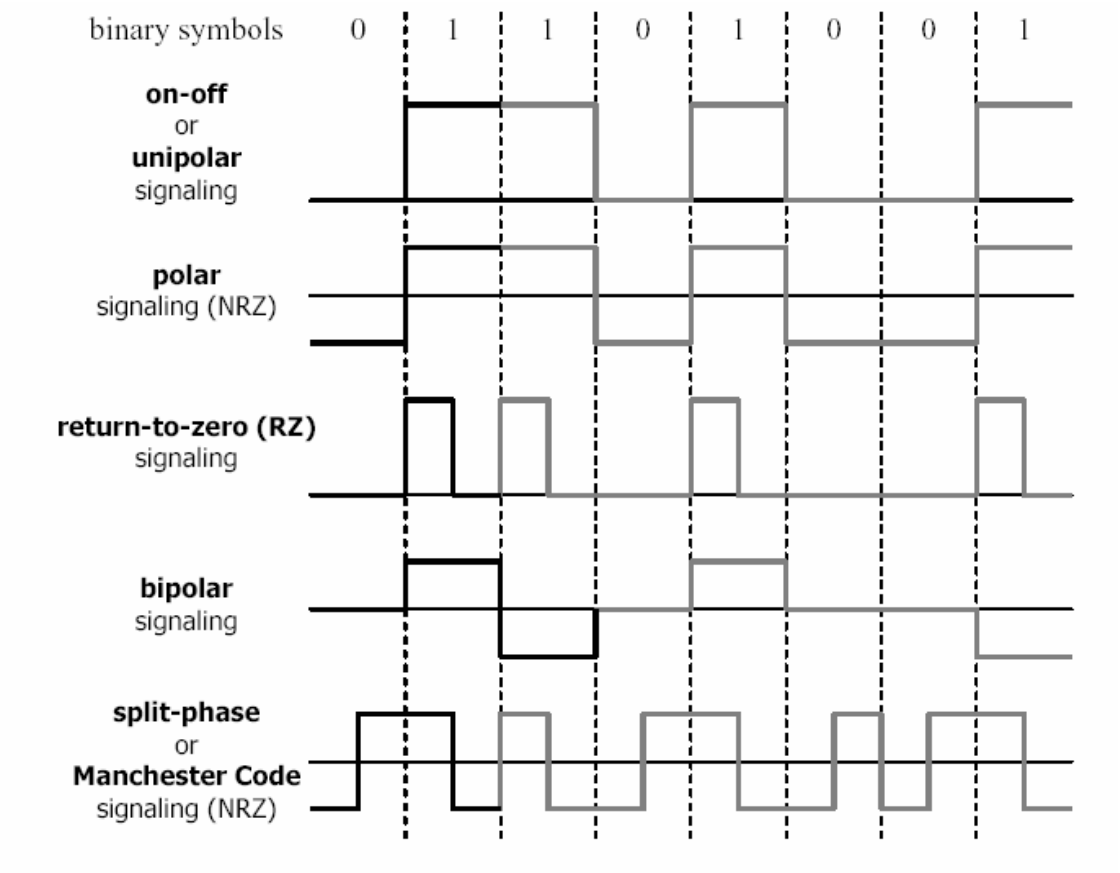


Figure 9. Binary coding.

F. SENSITIVITY OF THE READER

The signal that arrives at the reader needs to be sufficiently strong for it to be detected without errors. The sensitivity of the reader is an indicator of the required field strength (at the reader's input) for a signal to be received without errors. As a commonly accepted rule of thumb, the received signal should not be more than 100 dB below the level of the transmitted signal as shown in the figure below (Finkenzeller, 2003).

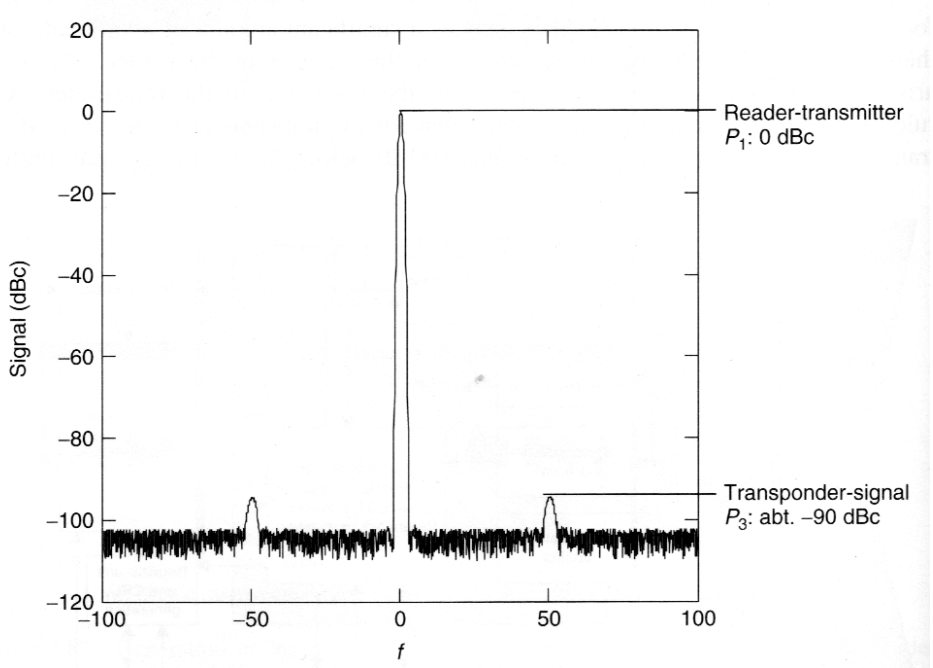


Figure 10. Relative power levels in a reader (from Finkenzeller, 2003).

The figure shows that the received signal is about 100 dB below the transmitted signal level.

G. CONCLUDING REMARK ABOUT LIMITATIONS

The immaturity of the technology is a contributing factor to the current limitations. Various solutions to mitigate existing problems have been developed, each with varying levels of success. The reliability of the technology is directly related to the performance of these solutions. Constant efforts to adapt and improve the solutions, as well as to come up with new ones will definitely help improve the reliability of the technology.

III. RELIABILITY ANALYSIS ON CURRENT TECHNOLOGY

A. OBJECTIVE

The objective of this study is to analyze the probability of obtaining an accurate read when a single RFID tag is in the interrogation zone of a reader. The probability of success (obtaining an accurate read) hinges on the quality of the readers and tags, as well as the limiting factors discussed in Chapter II. In this study, the readers and tags are assumed to be reliable, and functioning according to their specifications. The failure rate of these components will not be taken into consideration. Only the limiting factors that cause inaccurate tag reads will be considered.

B. METHODOLOGY

Inaccurate reads occur mainly because of the limiting factors. Relationships between the varying factors and the probability of obtaining an accurate read will be established. It is to be noted that most of the factors result in the attenuation of the signals, which will lead to a reduction in the SNR. SNR can be defined as $SNR = \frac{E_b}{N_0} = \frac{\frac{1}{2}A_{signal}^2}{\sigma^2}$ where A_{signal} is the signal amplitude, and σ^2 is the noise variance. Thus, we shall investigate the change in the probability of tag error as the SNR changes.

Simulink models will be built to study the effects that the varying factors has on the read reliability. The model will be detailed in section D. 500,000 tags each encoded with 2 bits of data will be made to transmit in succession. The data sent and data received will then be compared to determine if any tag error has occurred. The tag error rate for varying levels of SNR will be recorded.

C. FACTORS

The factors that affect the read reliability of RFID have been presented in Chapter II. This section examines each of these factors in greater detail, and determines how the signal level is attenuated as the factors vary.

1. Distance

As the distance d between the reader and the tag increases, the signal strength decreases. The electric field strength E is location dependent, and its magnitude decreases as the distance from the source increases. The following two equations shows that signal strength is attenuated by the cube and square of the distance for near and far field respectively (Lahiri, 2006):

$$\frac{E_1}{E_2} = \frac{d_2^3}{d_1^3} \text{ for near field}$$

$$\frac{E_1}{E_2} = \frac{d_2^2}{d_1^2} \text{ for far field}$$

If the distance between the tag and the reader is within one full wavelength, it is operating in the near field, otherwise it is operating in the far field. UHF and MW frequencies that operate in the far field region has a longer read range as compared to LF and HF communications that operate in the near field region.

A single frequency from each of the four bands was chosen, and their signal attenuation vs distance curves were generated.

Frequency Band	Frequency	Wavelength (m)	Typical operating region	Typical max range
LF	135 kHz	2222.22	Near field	50 cm
HF	13.56 MHz	22.12	Near field	3 m
UHF	869 MHz	0.35	Far field	9 m
MW	5.8 GHz	0.05	Far field	15 m

Table 3. RFID frequency ranges.

To determine the signal variation with respect to distance between the tag and the reader, it is assumed that the typical maximum range occurs at 50% of

the original signal strength (3 dB drop). For example, RFID system operating at LF (135kHz) would yield the following result:

$$\frac{E_1}{E_2} = \frac{d_2^3}{d_1^3}$$

$$\frac{E_1}{\frac{1}{2}E_1} = \frac{50^3}{d_1^3}$$

$$d_1 = 40cm$$

The maximum signal strength occurs at distances less than 40 cm. Beyond this distance, the signal starts to attenuate. The general formula for the signal strength E at any given distance *d* (cm) for RFID systems operating at this frequency can be expressed as:

$$\frac{E_{\max}}{E(d)} = \frac{d^3}{40^3}$$

$$\frac{E(d)}{E_{\max}} = \frac{40^3}{d^3}$$

The normalized signal strength vs distance curve for tags operating in the LF range is shown in the figure below. As the distance increases to beyond 50cm, the signal strength decreases rapidly.

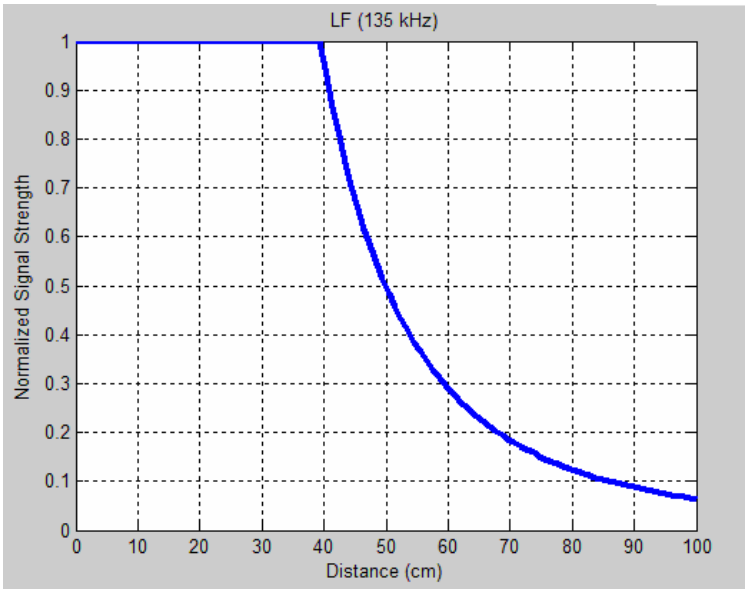


Figure 11. Signal attenuation at LF (135 kHz).

The normalized signal strength vs distance curves for HF, UHF and MW were similarly generated, and are shown by the following figures:

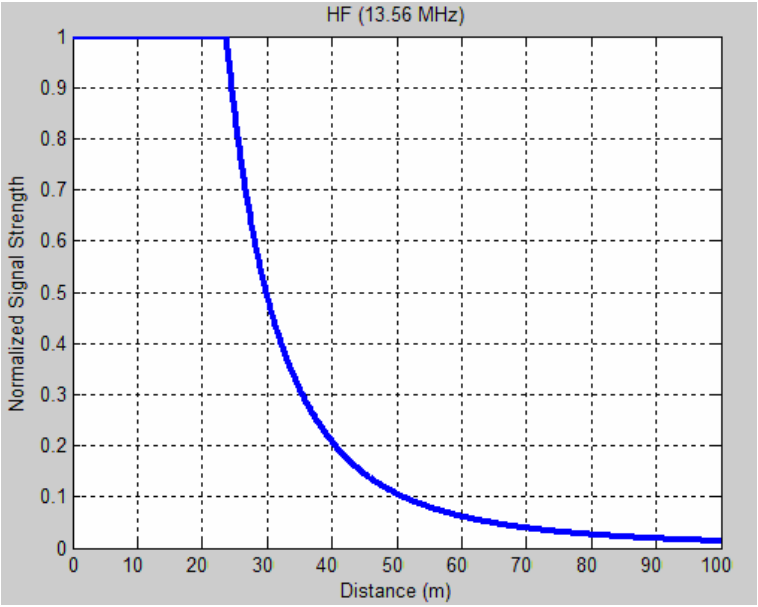


Figure 12. Signal attenuation at HF (13.56 MHz).

From the figure above, we see that severe signal attenuation starts to occur from about 2.5 meters for HF As for UHF (see figure below), the signal drop rapidly at distances greater than 8 meters.

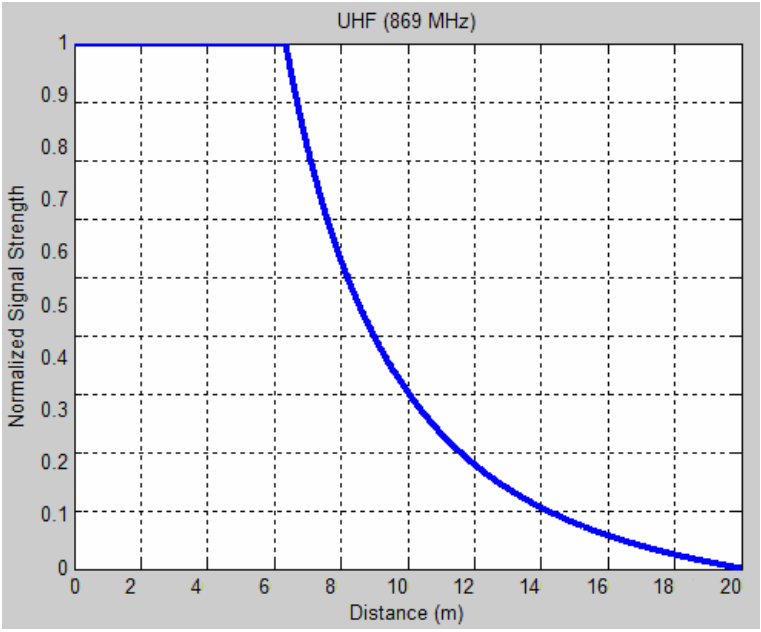


Figure 13. Signal attenuation at UHF (869 MHz).

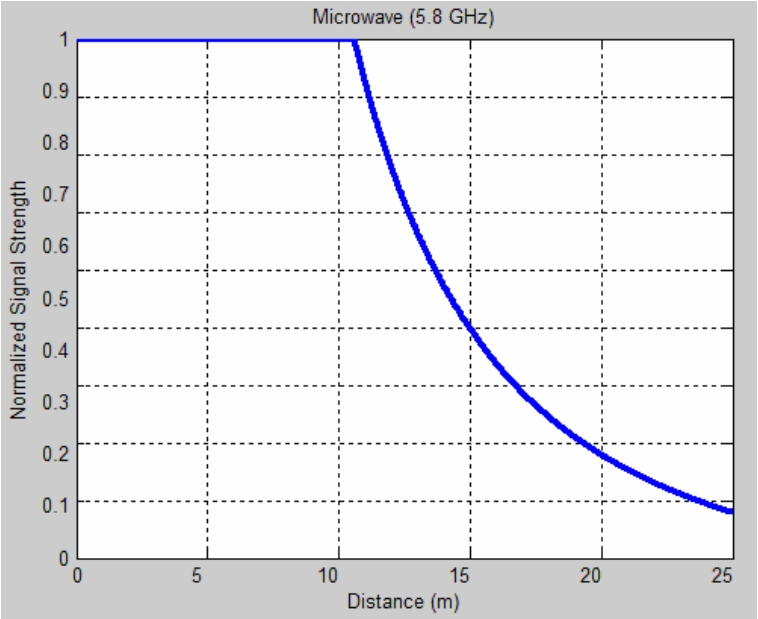


Figure 14. Signal attenuation at MW frequencies (5.8 GHz).

When the signal becomes attenuated, the SNR decreases, and hence, the probability of a read error increases. We can therefore deduce that the probability of an accurate read decreases with increasing distance.

2. Power

As the transmitted signal traverses the atmosphere its power level decreases at a rate inversely proportional to the distance traveled and proportional to the wavelength of the signal. Signal attenuation due to power transmission losses affect systems operating in the UHF and MW frequencies (Finkenzeller, 2003).

$$\text{Free Space Path Loss} = 20\log\left(\frac{4\pi r}{\lambda}\right)$$

The following figures show the increase in free space path loss as the distance traveled increases.

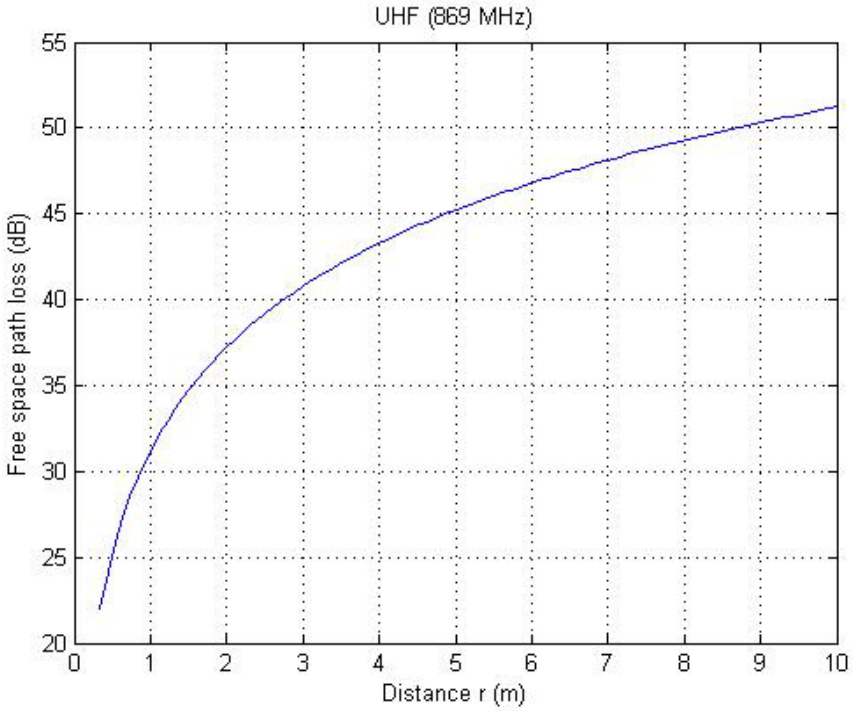


Figure 15. Free space path loss at UHF (869MHz).

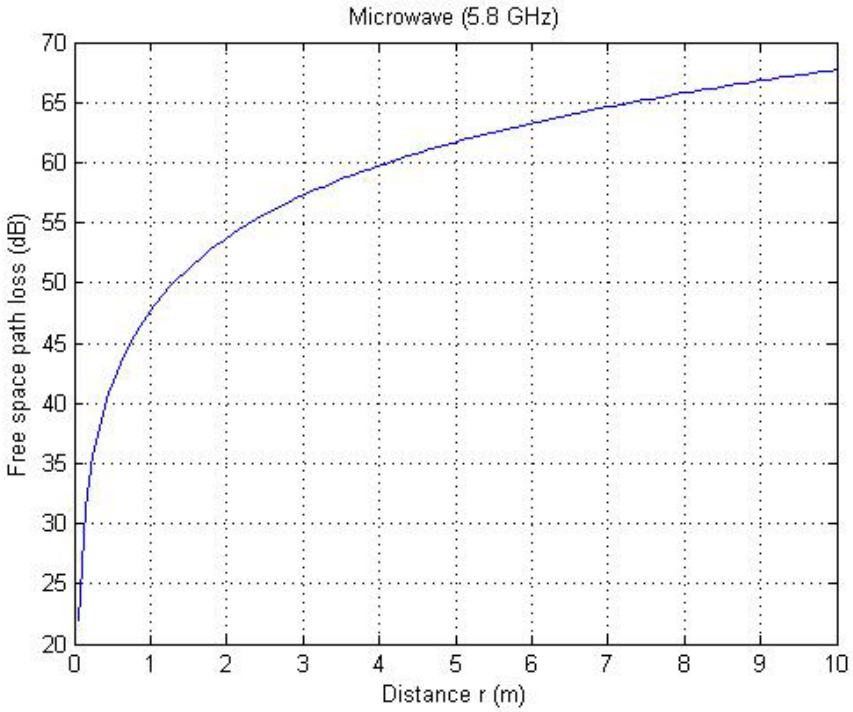


Figure 16. Free space path loss at MW (5.8GHz).

3. Environment

Noise effects in the environment can prevent RFID readers from getting an accurate read. The presence of wireless networks, or electronic devices such as motors and motor controllers, interferes with the RFID readers, decreasing the SNR. Noise is modeled as random Gaussian noise in our simulation models. We expect to observe that the probability of obtaining an accurate read decreases with decreasing SNR.

4. Orientation

The orientation of the tag affects the read reliability. Orientation sensitivity is most apparent when a linear polarized antenna is used. When the tag reader and antenna reader are aligned, the signal strength received is maximized. If the tag and reader antennas are misaligned, only a small portion of the energy emitted by the reader will hit the tag antenna, causing readability issues. Friis transmission formula gives the basis for this phenomenon (Jiang, 2006). The received power P_r corresponding to a transmit power P_t is determined by the wavelength λ and the distance d between the two antennas:

$$P_r = \frac{A_{et} A_{er}}{d^2 \lambda^2} P_t$$

where A_{er}, the aperture of the receive antenna is given by:

$$A_{er} = k \cos^2 \theta$$

k is a constant associated with the antenna's characteristics (such as effective height of the antenna and the intrinsic impedance of free space) and θ is the angle between the tag orientation and the propagating wave front from the reader.

From the above, we can deduce that the degradation due to orientation alone probably follows a $\cos^2 \theta$ variation.

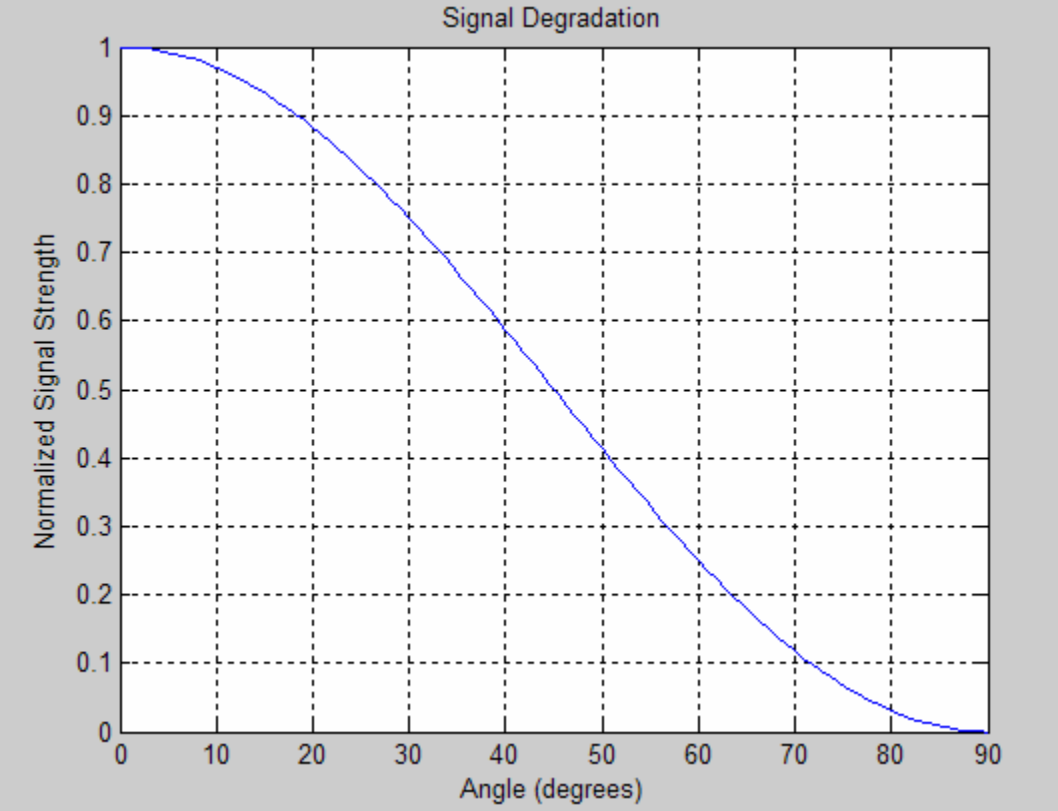


Figure 17. Signal degradation due to orientation.

Signal level is optimal when the tag is perpendicular to the polarization wave front. Signal level drops to half when the tag is rotated by 45 degrees. We can therefore deduce that the probability of an accurate read decreases with increasing deviation from the perpendicular orientation.

5. Encoding

Some methods of encoding are better than others in terms of error detection. The superiority of the Manchester coding as compared to the NRZ coding is evident in the case of a collision. Consider a tag using the NRZ encoding. Transponder 1 transmits the bit stream 10110010, while transponder 2 transmits 10011100. The signal received by the signal is 10111111, which does not correspond to either of the bit streams transmitted by transponder 1 or 2. The reader is not aware that an error has occurred - undetectable collision has occurred.

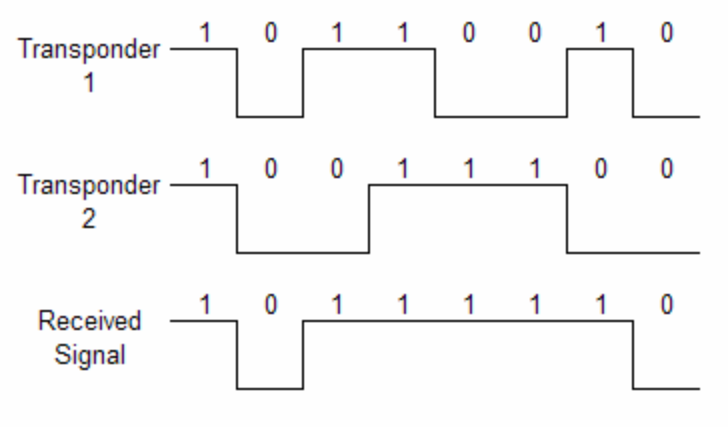


Figure 18. Undetectable collisions when NRZ coding is employed.

If Manchester encoding was used instead, collisions might result in a steady state period. As transitions have to occur in Manchester encoded signals, the steady state period that results is an indication that an error has occurred.

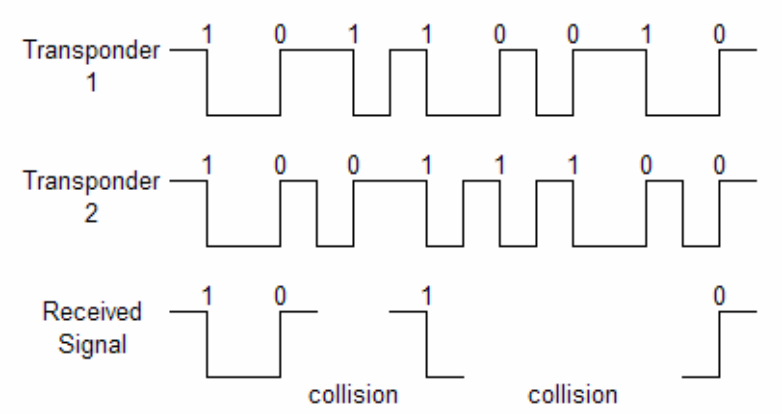


Figure 19. Collisions detected when Manchester coding is employed.

Other means of error detection that are commonly employed include the parity bit checking and the longitudinal redundancy check.

With parity bit checking, an extra bit is added to the string to be transmitted. Two parity check systems exist – the even parity or odd parity check. Both systems count the number of 1s in the bit string to be transmitted. If there is an even number of 1s, a 1 will be added if odd parity is used (so as to make the resultant total number of 1s odd), and a 0 is added at the end if even parity is used (so as to make the resultant total number of 1s even). Take the example of

10110100. With even parity, the following will be transmitted 101101000. With odd parity, 101101001 will be transmitted instead. Upon receipt of the signal, the receiver can verify that the number of 1s received is consistent with the parity bit. Note that the parity bit check can allow multiple errors to get by the system undetected. Suppose a 01 became a 10; a 0 became a 1 and a 1 became a 0; two 1s became two 0s – all these errors will not be detected by the parity bit check. In fact, transmission errors can even result in the parity bit itself being transmitted incorrectly. The probability of an undetected error can be calculated easily (Sklar, 2001). Take a 3 bit message as an example. With the parity bit appended, the codeword will be 4 bit long. The probability of an undetected error is equal to the probability that two or four errors occur anywhere in the codeword

$$P_{nd} = \binom{4}{2} p^2 (1-p)^2 + \binom{4}{4} p^4$$

where p is the probability of a bit error.

The longitudinal redundancy check (LRC) can be included on top of the parity bit checking. With LRC, the 1s (including the parity bit) are summed and appended at the end of the message block in a special field for error detection called the block check count (BCC). At the receiver end, the same addition is carried out and if the sum agrees with the BCC value received, the block is deemed error-free. Note however that even with the addition of the LRC, errors can still go undetected. Alternative means of error detection and correction needs to be explored.

6. Sensitivity of Reader

The sensitivity of a reader is usually defined with respect to a certain SNR or bit error probability (Nikitin & Rao, 2006). Precise sensitivity of a reader can be obtained through measurements. The sensitivity of a reader affects the read range achievable. Considering two readers, one with high sensitivity, and the other with low sensitivity, the reader with high sensitivity will be able to achieve a larger read range as compared to the reader with lower sensitivity. The figure below shows the limitations in read range due to reader sensitivity.

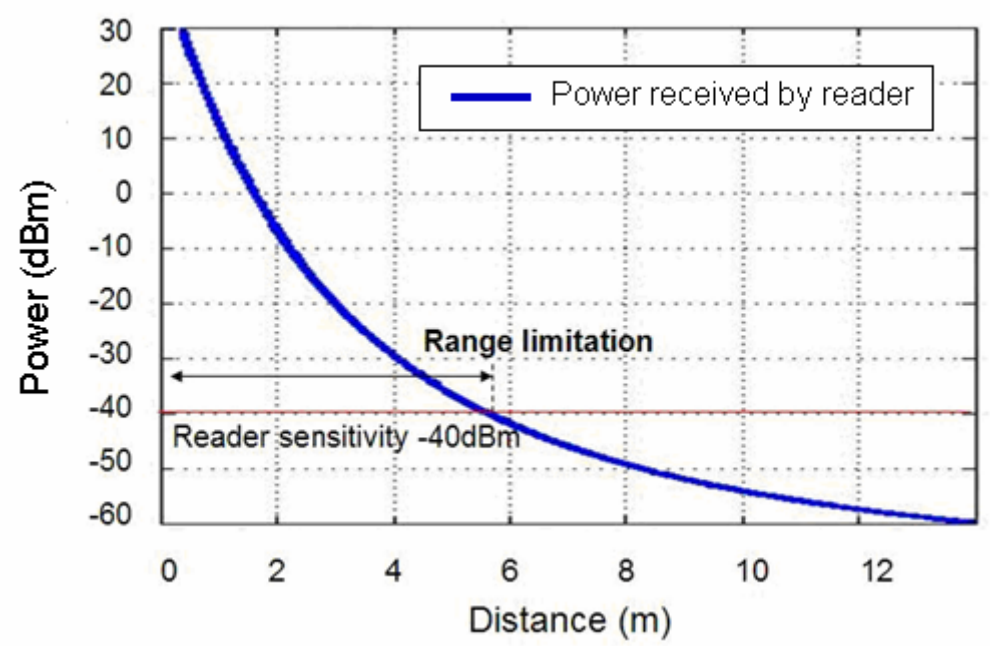


Figure 20. Range limitation due to reader sensitivity.

Suppose a reader emits a power of 1 Watt (30 dBm) and has a sensitivity of -40 dBm. As the distance between the reader and the tag increases, the power reflected back to the reader decreases. Due to the reader sensitivity, the range is limited to about 6 meters. If the reader sensitivity is -50 dBm, the read range can be increased to about 8 meters. Note that a typical square law envelope detector operating in the microwave range has a tangential sensitivity of about -45dBm, for which the detector will have an 8dB SNR.

A possible way to increase the read range is to increase the power emitted by the reader. Note however that the increase has to be within FCC's stipulated range.

D. THE MODEL

The Simulink® platform developed by MathWorks was used to build our models. An Intel Pentium M 1.6 GHz processor machine was used for our simulation runs. The following figure shows a block diagram of our model.

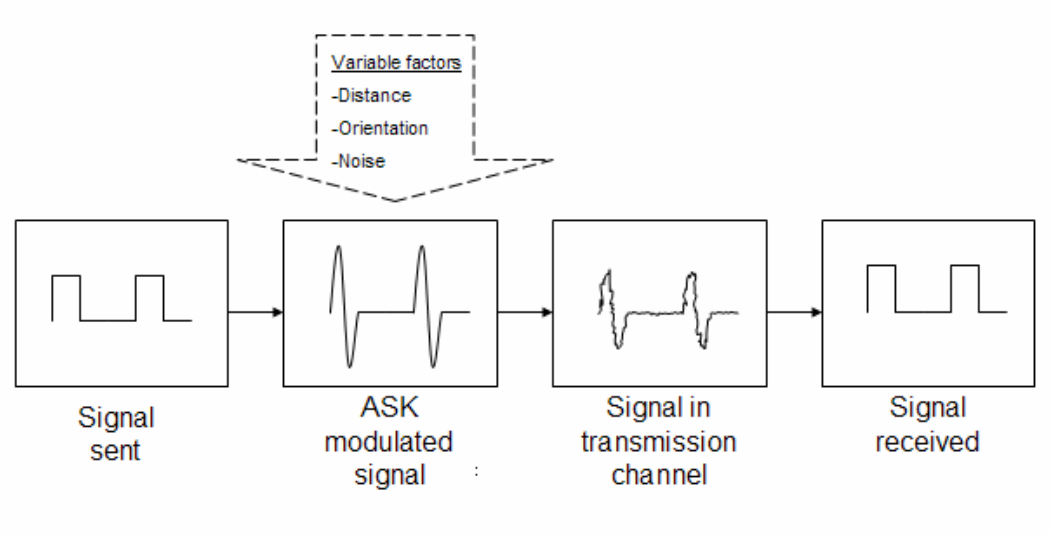


Figure 21. Schematic of simulation model.

The input data consists of binary 1s and 0s, which are modulated using amplitude shift keying (ASK). The signal power level can be adjusted, and the signal attenuation due to orientation or distance can be varied. Environmental noise is modeled in terms of random Gaussian noise. The signal that traverses the transmission channel is subsequently decoded to form the received signal.

For the first set of simulation runs, the data is coded using on-off keying (NRZ coding). Each run simulates 500,000 tags transmitting in succession, with each tag transmitting 2 bits of data. The data sent and received are compared and the number of tags read correctly determined, thereby obtaining the read reliability under the varying factors.

Note that although the model takes into account 2 bits of data, the results can be scaled upwards and made to be applicable to tags of larger capacity. The simulations determine the bit error probability P_b at varying SNR. With these bit

error probability results, the tag error rate (TER) at a particular SNR for a tag containing *n* bits of data can be calculated as follows:

$$TER = 1 - (1 - P_b)^n$$

Tag capacity can be as large as 96 bits. Simulation models for 96 bit tags can be built, but such simulations become computationally challenging in terms of computational time and memory. A simple extension of the results using the equation above might be more efficient in such cases.

The screen shots below show the data sent, modulated and received in the ideal case where no errors in transmission occur.

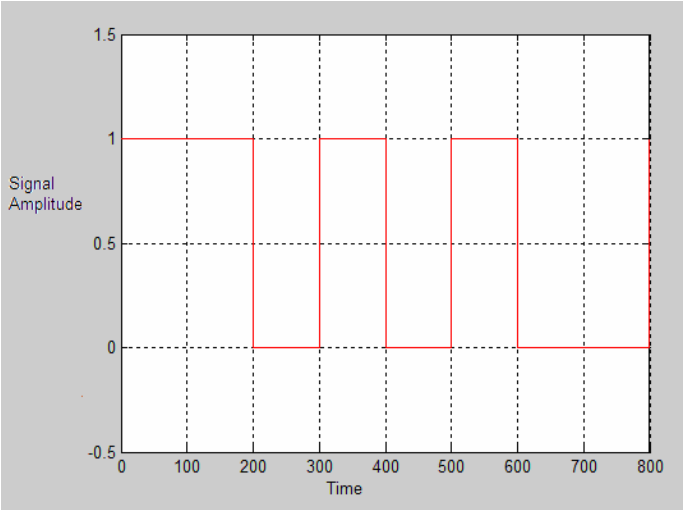


Figure 22. Tag data sent.

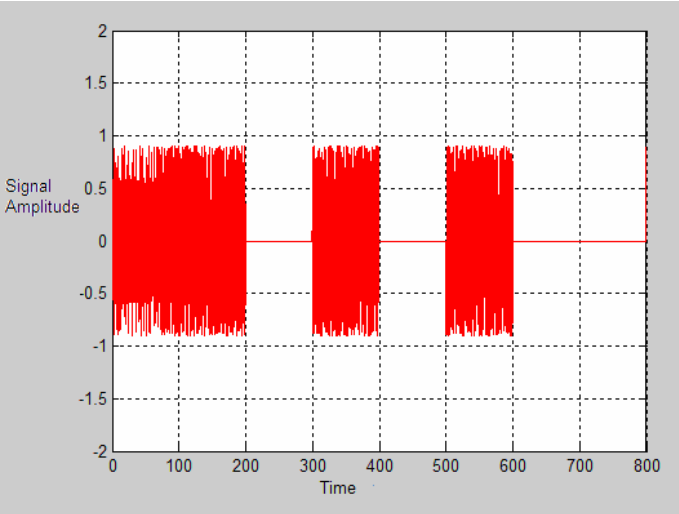


Figure 23. ASK signal.

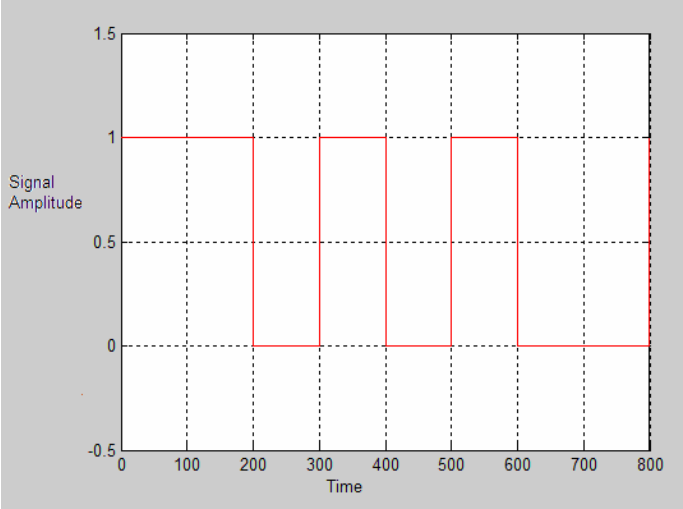


Figure 24. Tag data received.

E. PERFORMANCE ANALYSIS & RESULTS

The bit error probability of our Simulink model at varying SNR was determined. The simulation results correlate closely with the theoretical bit error probability for noncoherent detection, thus confirming the integrity of our simulation model.

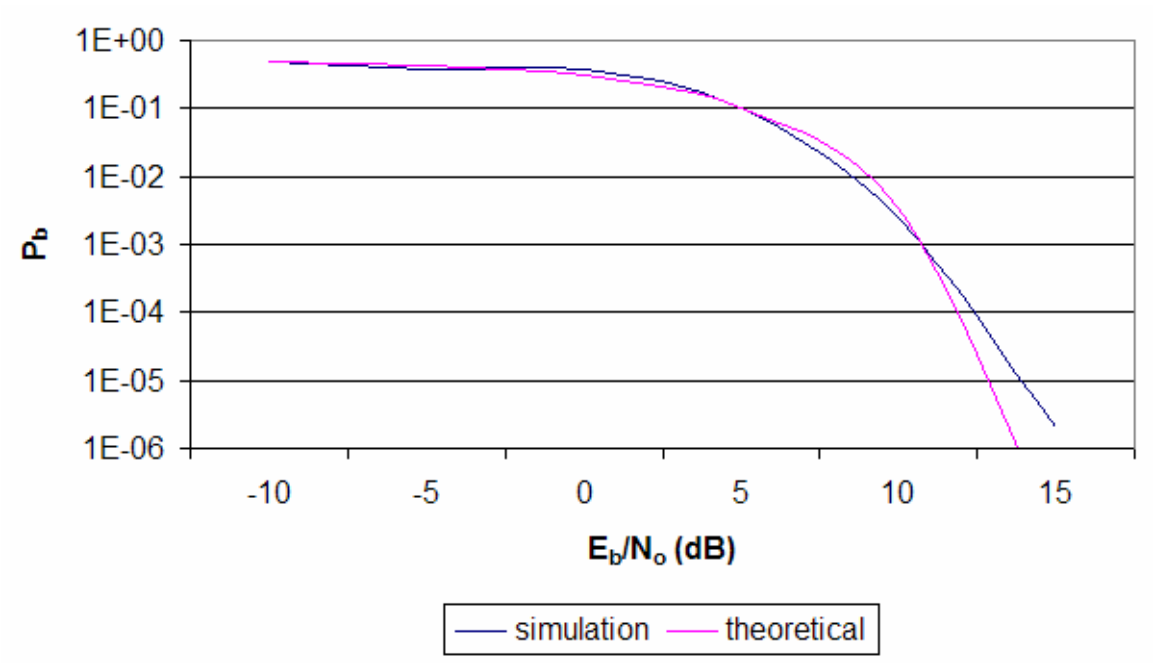


Figure 25. Simulation results showing the bit error probability for noncoherent detection of OOK signals.

Subsequently, the tag error rates (TER) for varying numbers of data bits stored per tag was determined. As long as one or more of the data bits stored on a tag is in error, the tag is considered to be read in error. Given that *n* is the number of bits stored on a tag, the tag error probability can be expressed as follows:

$$P_{\text{tag error}} = 1 - (1 - P_b)^n$$

Clearly, as the number of bits stored per tag increases, the tag error probability increases. The figure that follows shows the tag error probabilities for varying amounts of information stored on a tag.

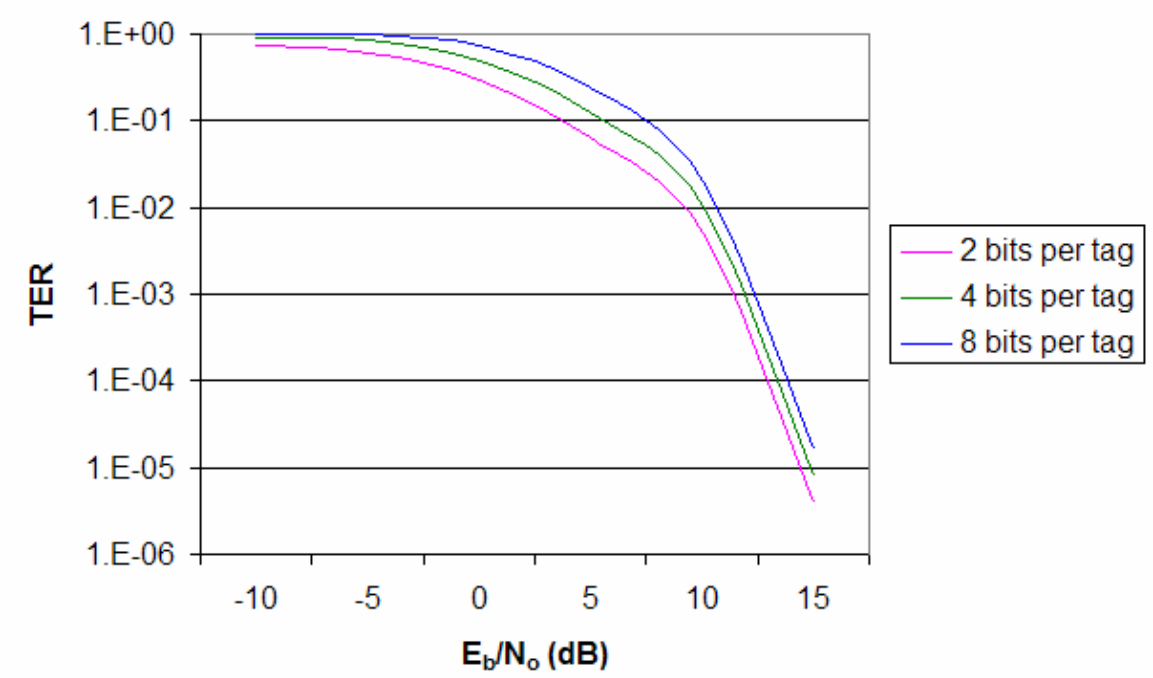


Figure 26. Simulation results showing the tag error rates for varying numbers of data bits stored per tag.

Depending on the application in which it is deployed, a typical passive tag can contain a few bits to hundreds of bits for data storage (Lahiri, 2006). An *n* bit tag provides up to 2^n unique identifiers. Hence, for an 8 bit tag, 256 unique identifiers are available. If more unique identifiers are required, *n* has to increase, inevitably leading in an increase in tag error rate.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. IMPROVING THE RELIABILITY OF THE TECHNOLOGY USING CODE SHIFT KEYING

The read reliability of RFID can possibly be improved through a variety of ways. This section explores the use of various coding techniques to achieve higher read reliability. One family of codes worth considering is error detection and error correction codes. Error correction coding is the means whereby errors which may be introduced into digital data as a result of transmission through a communication channel can be corrected based upon received data (Moon, 2005). The performance of the repetition code will be studied in this section. In addition, another modulation technique, namely, Code Shift Keying will also be explored.

A. REPETITION CODE

One of the simplest error correcting code is the repetition code. Instead of sending out the data bit once, each data bit is repeated n times, where *n* is an odd integer. Suppose [1 0 1 1] is to be sent. A repetition code with *n* = 3 will result in the transmission of [1 1 1 0 0 0 1 1 1 1 1 1] instead. Simple majority voting of the received bits (hence the reason for the odd number) determines the transmitted bit more accurately than sending it alone. Suppose that the received vector is [1 0 1 0 0 1 0 1 1 1 1 1]. Although some of the bits are transmitted incorrectly, the decoded value will still be [1 1 1 0 0 0 1 1 1 1 1 1] based on majority logic decoding. Note that the bit stream emerging from the repetition channel coder has data rate *n* times higher than that of the original bit stream.

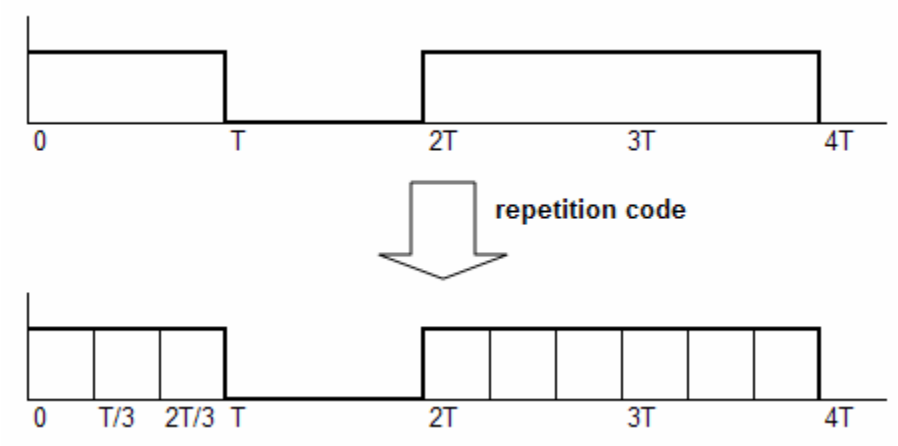


Figure 27. Repetition code.

1. Performance Analysis of Repetition Code

A simulation was carried out to evaluate the performance of the repetition code. The results are plotted in the figures below. As *n* increases, the probability of error decreases sharply. In the case where the probability of a single bit error, P_b is 0.2, we see that the probability of error drops to almost half when *n* is 3.

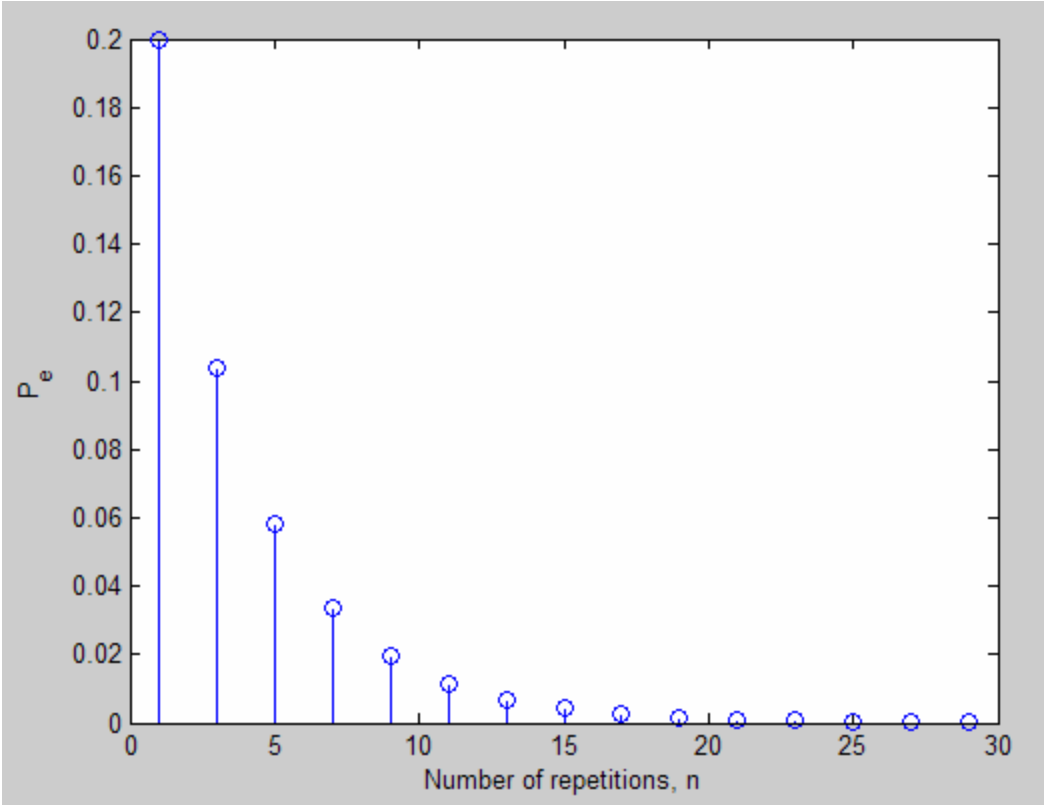


Figure 28. Performance of repetition code.

The results of the simulation are consistent with what we expect to achieve. An error occurs when more than $\frac{n+1}{2}$ of the transmitted symbols are received in error. Hence, the probability of error can be expressed as follows (Lin & Costello, 2004):

$$p_e = \sum_{k=(n+1)/2}^{n} \binom{n}{k} (1-P_b)^{(n-k)} P_b^k$$

The bit error probability curves with repetition (n=5) and without repetition are shown in the figure below.

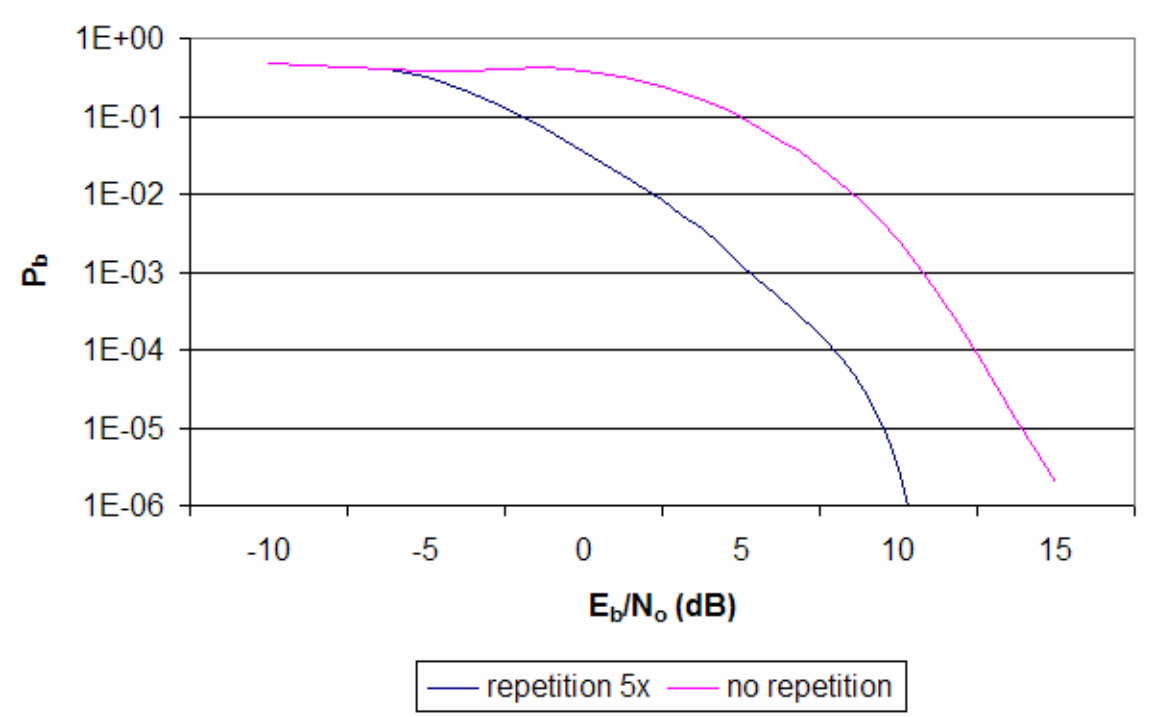


Figure 29. Simulation results showing the improved performance when repetition code is utilized.

For a bit error rate $P_b=10^{-4}$, an improvement of close to 4 dB is observed. As the number of repetitions increases, the performance will improve further. However, the bandwidth requirements increase proportionately as well. There is a trade off between bandwidth and probability of bit error.

B. CODE SHIFT KEYING

Code shift keying utilizes a set of $M = 2^k$ orthogonal sinusoidal Walsh functions to represent a set of *M* distinct *k*-bit symbols where *M* is a power of 2 (Ha, 2006). Walsh functions take the values of 1 and -1 only, and can be obtained from the Hadamad matrix given by

$$H_M = \begin{bmatrix} H_{M/2} & H_{M/2} \\ H_{M/2} & -H_{M/2} \end{bmatrix}$$

The four-ary Walsh function can be obtained recursively as follows

$$H_1 = 1$$

$$H_2 = \begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

A CSK modulator demultiplexes the input bits to form symbols, which are transformed to corresponding Walsh functions.

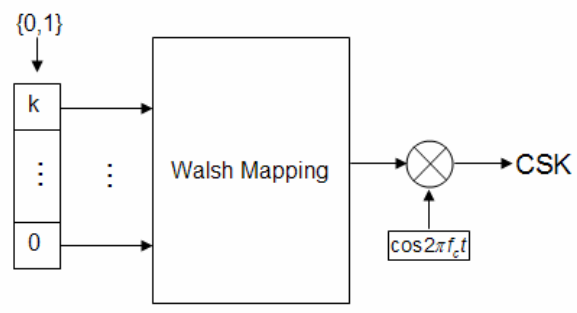


Figure 30. CSK modulator.

A 2-bit data will be transformed to Walsh functions with four-chips. Suppose [0 1] is transmitted. This data will be transformed to [1 -1 1 -1].

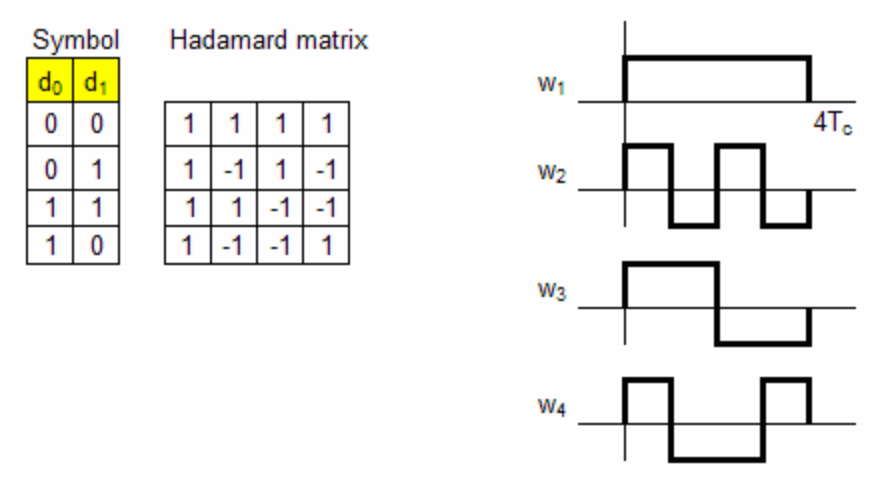


Figure 31. Four-ary Walsh functions.

A four-ary Walsh function has 4 unique 'code words' (w_1, w_2, w_3 and w_4). If the received sequence deviates from any of these 4 possibilities, the demodulator is able to determine which of these 4 was actually transmitted by using a maximum detector. This technique is commonly known as 'hard-decision demodulation'. The receiver makes a best estimate of the original symbol that gave rise to the particular transmitted waveform (Gardner & Baker, 1997). This ability is more appreciably demonstrated as *k* increases.

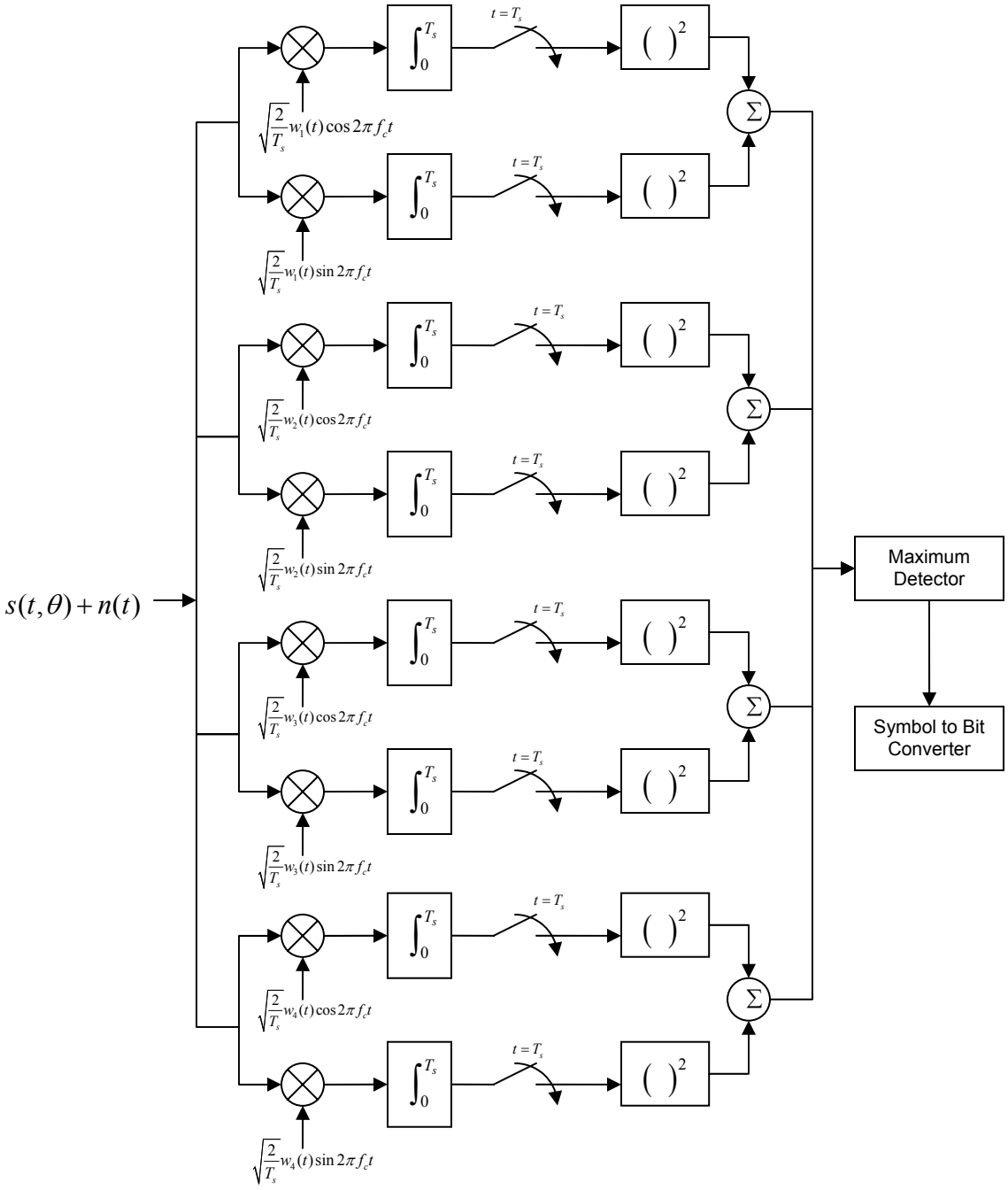


Figure 32. 4-ary CSK Demodulator.

For the purposes of this study, the four-ary Walsh function will be investigated. Note that these results can be extended to higher order Walsh functions.

A Simulink model of the CSK demodulator is built and its performance was studied. The implementation of the demodulator in Simulink® follows the circuit diagram shown in figure 32. The input signal is convolved with the sine and cosine components of each of the four walsh functions, integrated, squared, and results compared using a maximum detector to determine the most likely signal sent.

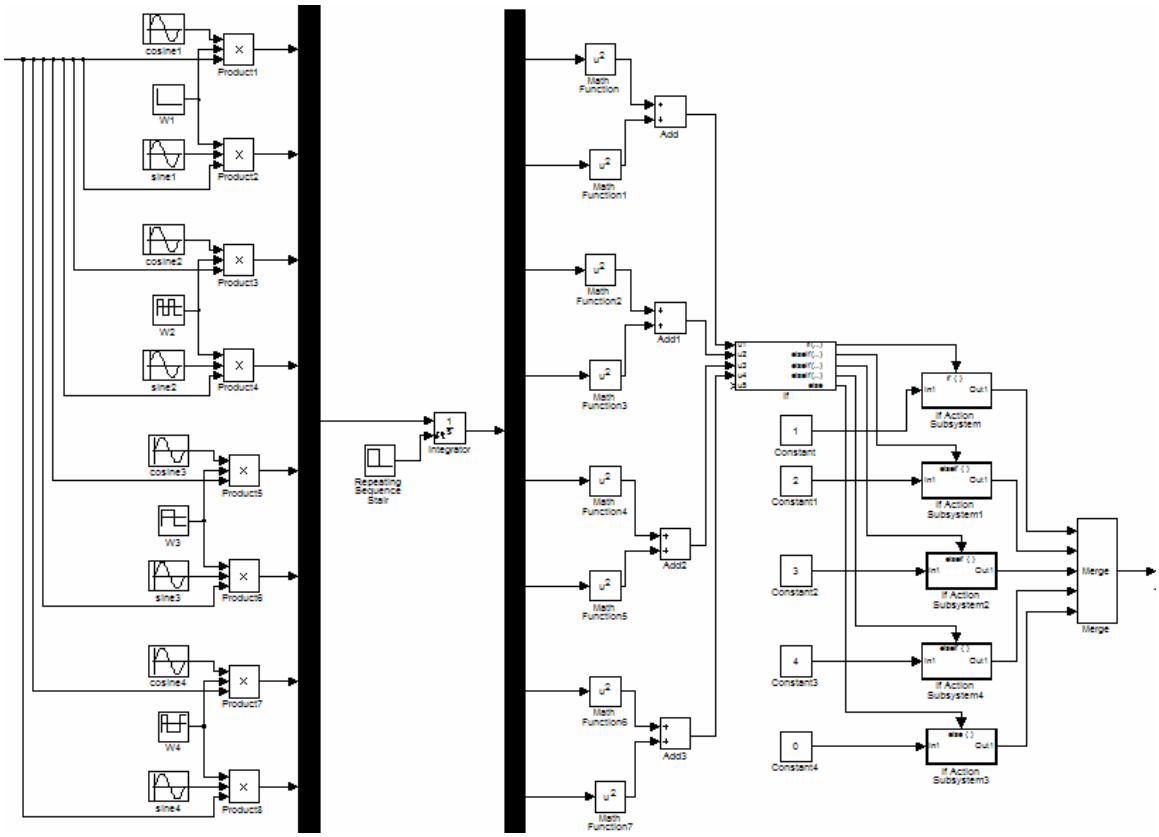


Figure 33. Simulink model of CSK demodulator.

1. Performance Analysis of Code Shift Keying

The bit error probability at varying levels of SNR generated by our simulation model was compared with the bit error probability of noncoherently detection of orthogonal 4-FSK signals (see figure 34). The simulation showed that a SNR of 5 dB is required for a bit error probability of 1×10^{-2}, while a SNR of 5.6 dB is required in theory. The comparisons showed close correspondence, thus confirming the integrity of our simulation model.

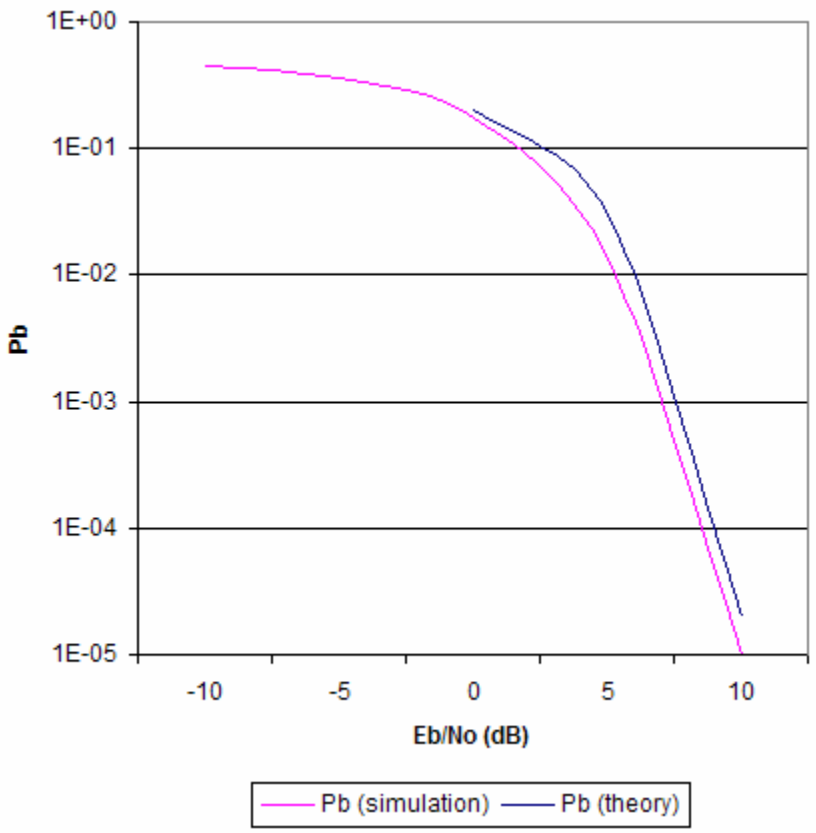


Figure 34. Comparison of simulation results with theoretical results for noncoherent. detection of CSK signals.

Subsequently, the tag error rates at varying SNR was obtained. The results for a 2 bit tag is shown in the figure below. Similar to what was shown with the OOK case, we expect the tag error probability to increase as the number of bits stored per tag increases.

The simulation results obtained using CSK was compared with that obtained using OOK. At a tag error rate of 10^{-5} dB, an improvement of close to 4 dB is observed (see figure below).

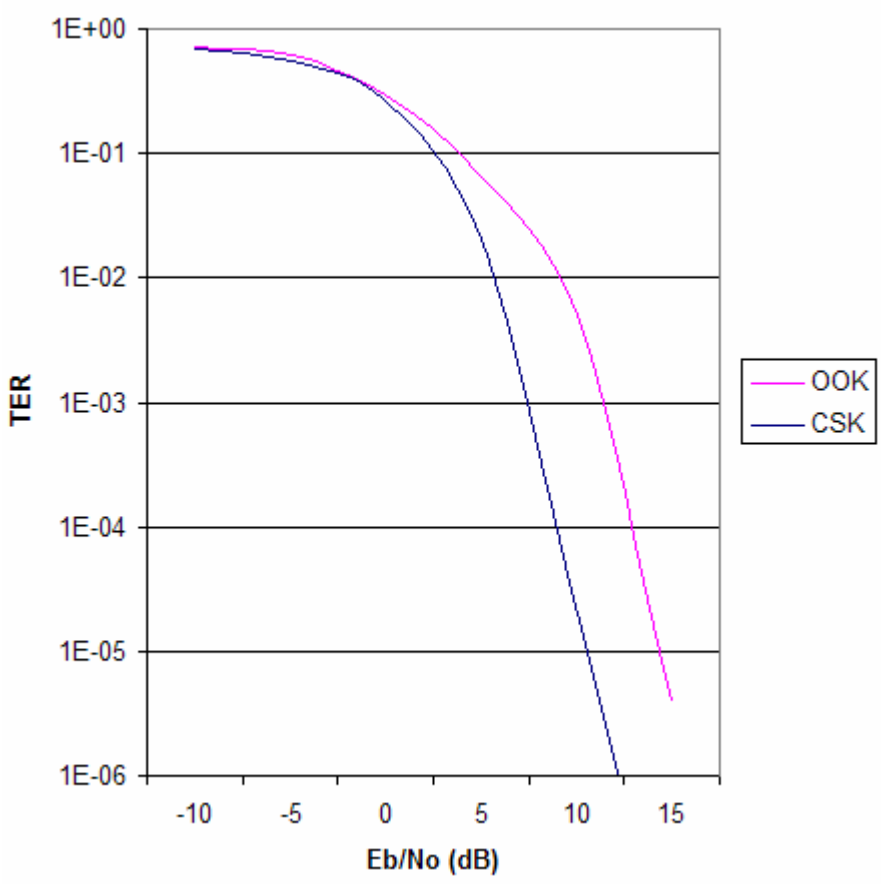


Figure 35. Comparison of OOK and CSK for a 2 bit tag.

CSK is clearly a more superior method of modulation as compared to OOK. Higher read reliability can definitely be achieved with this modulation technique.

C. REPETITION CODE & CODE SHIFT KEYING

Given the advantages of both techniques, it is worth exploring the impact of combining both techniques.

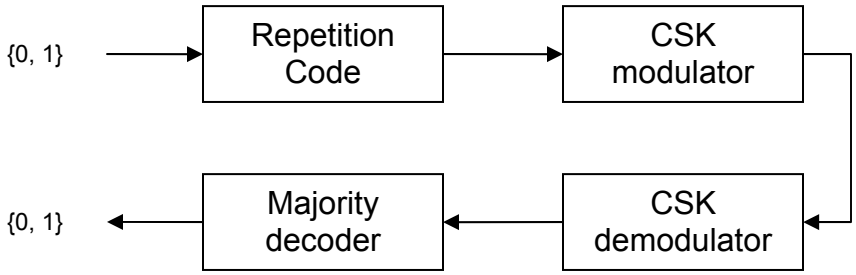


Figure 36. Block diagram of system.

Tag data is repeated an odd number of times, and modulated using code shift keying. The same method of noncoherent demodulation applies; the decoded sequence is passed to the majority decoder, which will attempt to correct errors in the same way as described in the preceding section.

1. Performance Analysis of Code Shift Keying with Repetition

The input bits are repeated 5 times before being passed to the Walsh mapper for modulation. The results of the simulation are shown in the figure below. The results obtained in section B is plotted in the same graph for comparison.

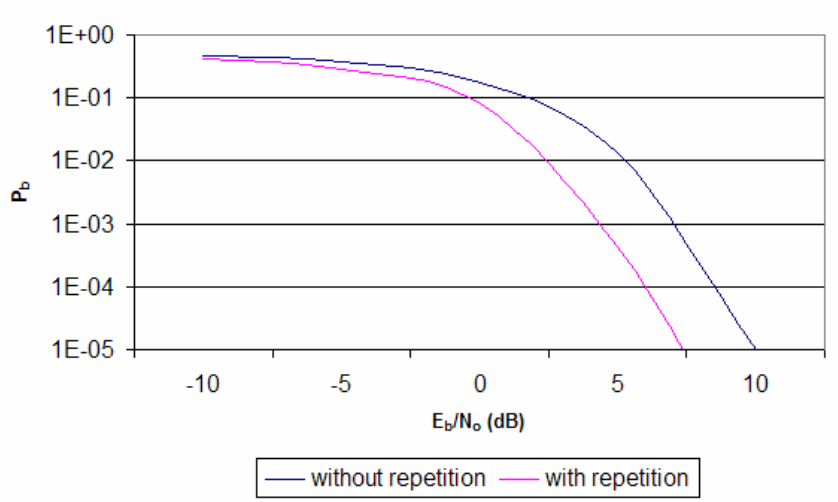


Figure 37. Comparison of CSK BER with and without repetition code.

An improvement of 2.5 dB is observed. A bit error probability $P_b=10^{-5}$ can be achieved at an E_b/N_o of about 7.5 dB as opposed to 10 dB without repetition.

D. PERFORMANCE ASSESSMENT

The bit error rate performances of all the four coding and/or modulation variations are presented in the following figure for comparison. Our simulations revealed that with OOK, an SNR of 12.5 dB is required to achieve a bit error rate of 10^{-4}. Often, due to environment conditions and limitations in terms of orientation of tags or other uncontrollable factors, this SNR is not attainable. As such, a sufficiently high read reliability of the tag is not possible. The CSK with repetition coding technique allows us to achieve the same bit error rate performance at a lower SNR. With the use of the repetition code, it was found that performance improved by about 4 dB when each bit is repeated 5 times. This means that an SNR of 8.5 dB is sufficient to achieve a bit error rate of 10^{-4}. With the use of CSK, a significant improvement in performance was observed. To achieve a bit error rate of 10^{-4}, an SNR of about 8.5 dB is required. Repetition of bits before code shift keying showed more improvements in performance. Simulation results showed a 2.5 dB improvement as compared to when no repetition was used. This means that an SNR of 6 dB is sufficient to achieve a bit error rate performance of 10^{-4}.

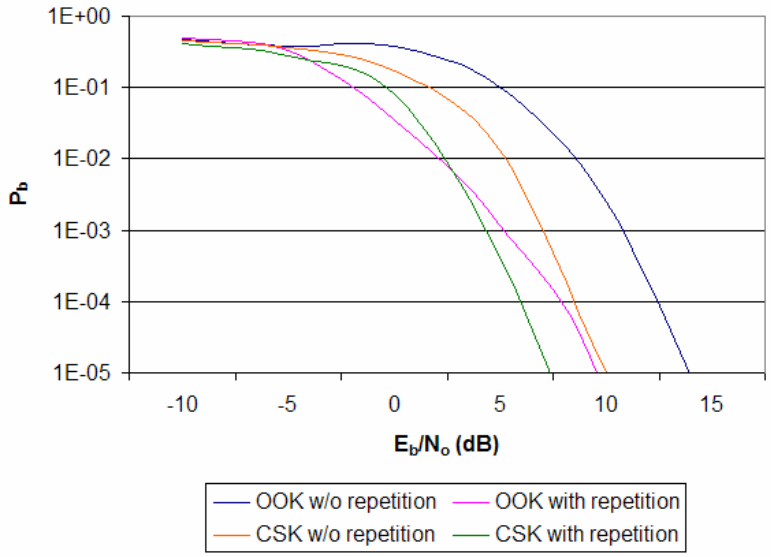


Figure 38. Comparison of BER Performance.

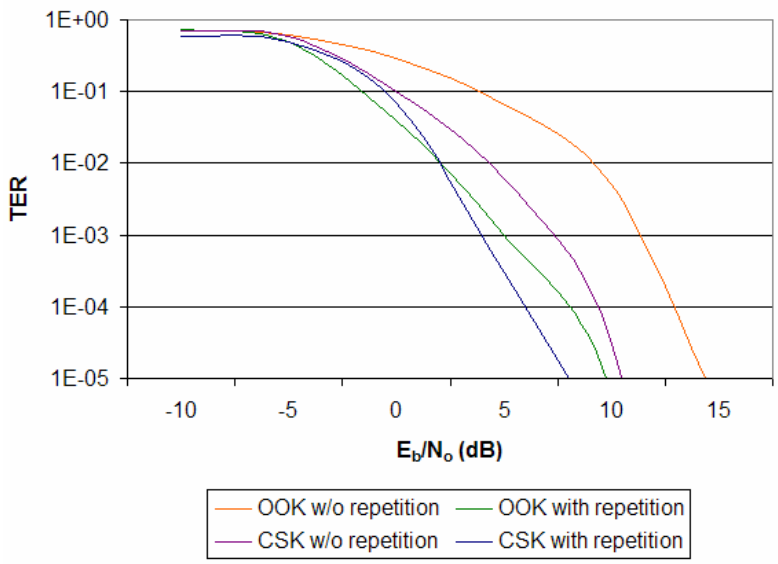


Figure 39. Comparison of TER Performance for a 2 bit tag

The tag error rates for 2 bit tags are shown in the figure above. All the curves are shifted to the right by about 0.3dB. As the number of bits stored in a tag increases, a higher SNR will be required to obtain the same performance.

Evidently, CSK with repetition code is able to provide significant improvements in the bit error rate performance, and hence, increase the probability of accurate reads, thereby making the RFID system more reliable.

V. APPLICATION OF RESULTS

The simulation runs revealed that the alternative modulation/coding techniques proposed are able to achieve better bit error rate (BER) performance as compared to the coding technique used in most existing RFID systems. This improved BER performance translates to a higher read reliability.

This chapter examines the impact that the improved performance has on the overall RFID system, in terms of tag orientation, reader placement, as well as the distance between adjacent tags.

In doing this, the U.S. Department of Defense (DoD) RFID policy will be examined, and a specific case study will be used.

A. U.S. DEPARTMENT OF DEFENSE RFID POLICY

The U.S. Department of Defense (DoD) officially released its RFID policy on July 30, 2004. The policy stipulates that starting January 1, 2007, all commodities and commodity pallets shipped to any DoD facility must have RFID tags.

Pertinent points from the policy include the following:

- Passive tags to be attached to pallets, cases and items (see figure)

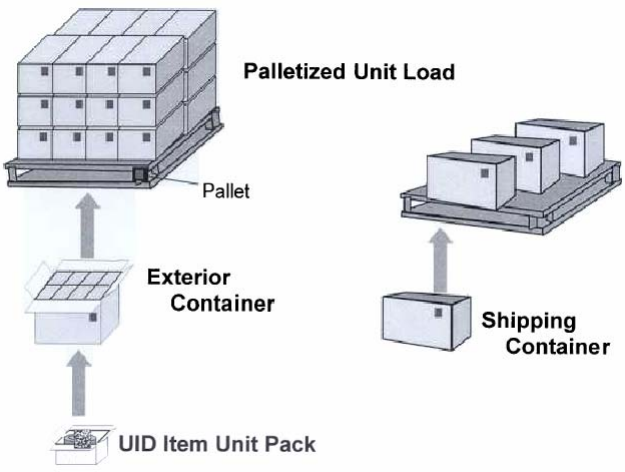


Figure 40. Tagging of pallets, cases and items (from US DoD RFID Policy).

- Approved frequency range for passive RFID implementation is UHF 860-960MHz
- Supplier can use either the EPC[1] or UID[2] data format to encode item identity, each tag having a data capacity of either 64 bits or 96 bits
- For palletized unit load passive RFID tags, passive RFID tags on shipping containers, and exterior containers within palletized unit load, and the UID item unit pack passive RFID tags that are passing through a portal, the read distance shall be at least 3 meters, reading passive RFID tags at about 25 meters per minute (e.g. forklift)
- For individual shipping container passive RFID tag, an individual exterior container passive RFID tag, and the UID item pack passive RFID tag moving on a conveyor, the read distance shall be at least 1 meter, reading passive RFID tags at about 0.3 meters per minute
- In addition, the Suppliers Information Guide provides guidelines on where the RFID tags should be placed (see figure below)

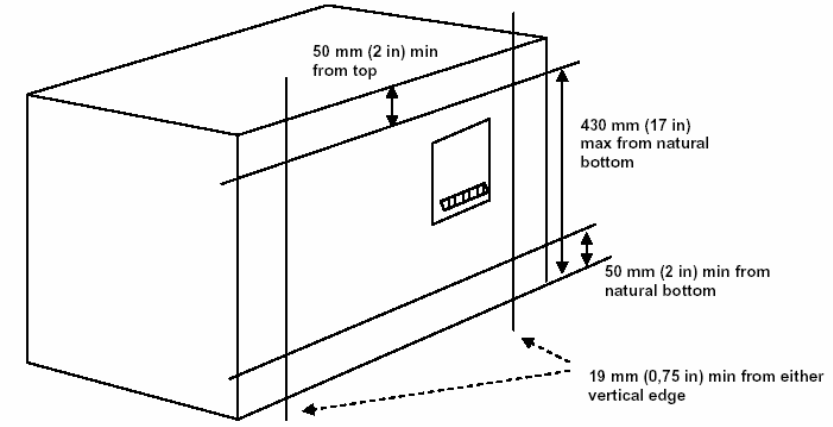


Figure 41. RFID tag placement on a case (from US DoD Suppliers' Passive RFID Information Guide).

[1] Electronic Product Code (EPC) is a unique number that can identify the manufacturer, product, version, and serial number. The EPC also provides an extra set of digits to identify unique items.

[2] Unique Identification (UID) is a unique "part identifier" that contains data elements used to track DoD parts through their life cycle.

B. CASE STUDY

This section evaluates the impact that our simulation results have in meeting DoD's guidelines for cases moving on a conveyor belt. DoD's requirements are summarized in the table below.

Operating range	UHF (860 to 960MHz)
Minimum read distance	1 meter
Power	Maximum 1 Watt (FCC regulations)
Speed	0.3 meters per minute
Storage capacity	At least 64 bits

Table 4. DoD requirements for case moving on a conveyor belt.

The maximum range for systems operating in the UHF range is typically 9m. Our analysis showed that signal starts to attenuate at distances beyond 6m (see figure 13). If the reader is placed less than 6m from the conveyor belt, signal attenuation due to distance will be minimal.

The free space path loss for UHF systems operating at a range of 1 meter is about 30 dB (see figure 15). As the distance increases to 9 meters, this value increases to 50 dB. In order to maximize the SNR to obtain a higher probability of an accurate read, the distance between the reader and conveyor belt should be minimized as far as practicable.

Where orientation is concerned, signal attenuates by 50% when the tag reader and antenna are misaligned by 45 degrees (figure 17). Care should be taken to ensure that tags are not misaligned by more than 45 degrees, as signals will be severely attenuated beyond that point.

The speed at which the conveyor belt is moving is stipulated as 0.3 meters per minute. Tag read rates[3] are typically in the order of milliseconds, and hence,

[3] Read rate is defined as the maximum rate at which data can be read from a tag.

the speed of the conveyor belt is sufficiently slow to allow for data transfer between tags and readers. However, it is to be noted that the chances of obtaining accurate reads are higher when only one tag is present in the reader's interrogation zone at any one time. As such, there is a need to ensure that adjacent tags are placed sufficiently far apart on the conveyor belt if we want to ensure that no more than one tag is in the reader's interrogation zone at any one time.

Consider the distance *y*, which affects the beam spread. As the distance *y* is increased, the beam spread *w* increases. If the items on a conveyor belt are not spaced far enough (separation distance *x*), two tags might enter the interrogation zone of the reader at any one time, resulting in possible collisions.

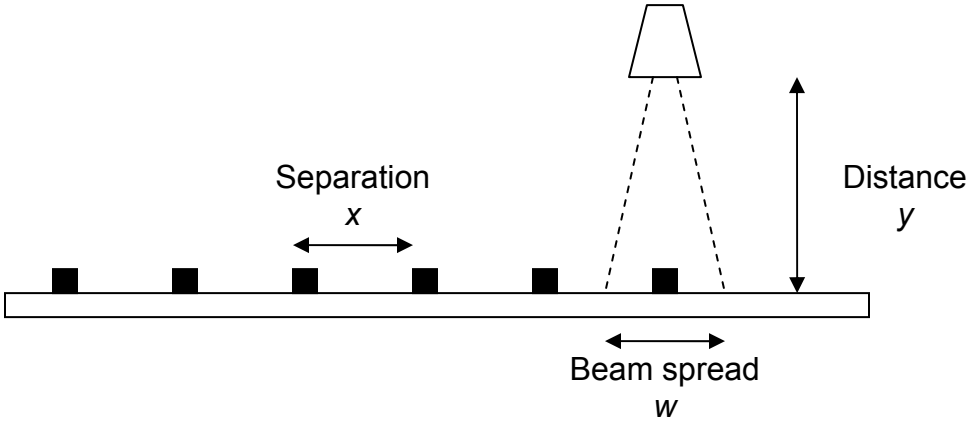


Figure 42. A possible application – items on a moving conveyor belt.

The beam spread is determined by the beamwidth[4] of the antenna as well as the distance *y*. Assuming that distance *y* is 1 meter, and the beamwidth is 30 degrees, we can determine the beam spread using trigonometry.

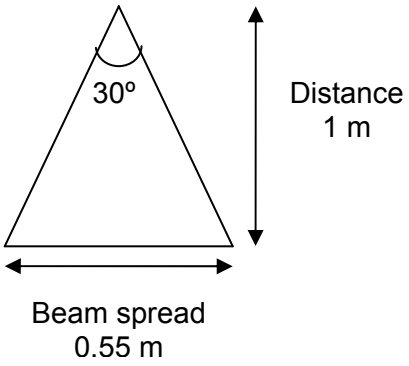


Figure 43. Beam spread calculation using trigonometry.

To ensure that there is only one tag in the interrogation zone at any one time, the separation distance should always be larger than the beam spread, that is $x \geq w$. Note that the above is a simplified case. In reality, the RFID tag might not be in the same position all the time. The item on which the tag is mounted might be rotated. This complicates the issue and care must be taken to determine the optimal spacing between items.

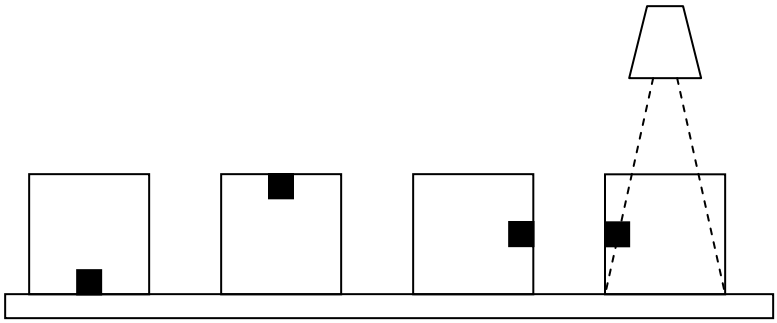


Figure 44. Tagged objects on a conveyor belt oriented in different directions.

If the separation of the items allows tag collisions to occur, the time taken to read the tags will increase, and the probability of a read error will also increase.

[4] Beamwidth is defined as the angle between the half-power (3 dB) points of the main lobe when referenced to the peak power of the main lobe. Can be calculated (or measured). Depends on antenna's maximum dimension as well as wavelength.

Taking into account the factors presented above, the following figure shows the ideal orientation of tags with respect to the reader antenna.

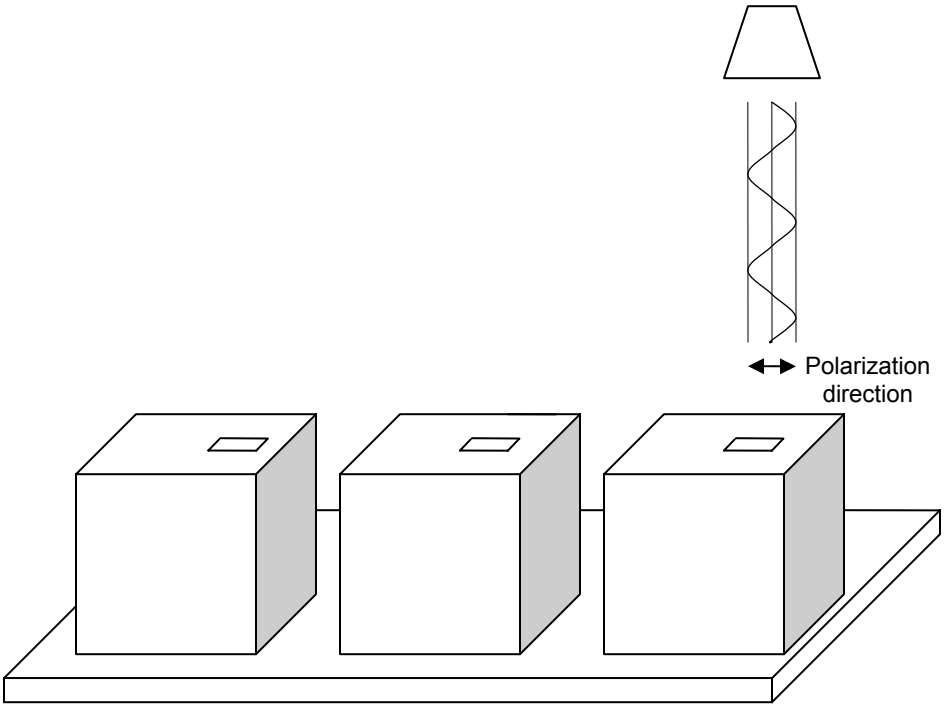


Figure 45. Proper tag orientation for a linear polarized antenna.

Similarly, taking into account all the factors presented above, the following figures show the optimum allowable separation to maximize the probability of obtaining accurate tag reads at varying ranges.

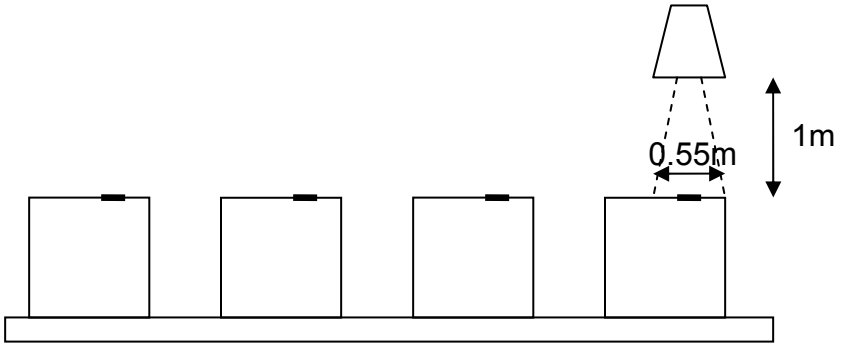


Figure 46. Minimum separation distances when range is 1 meter.

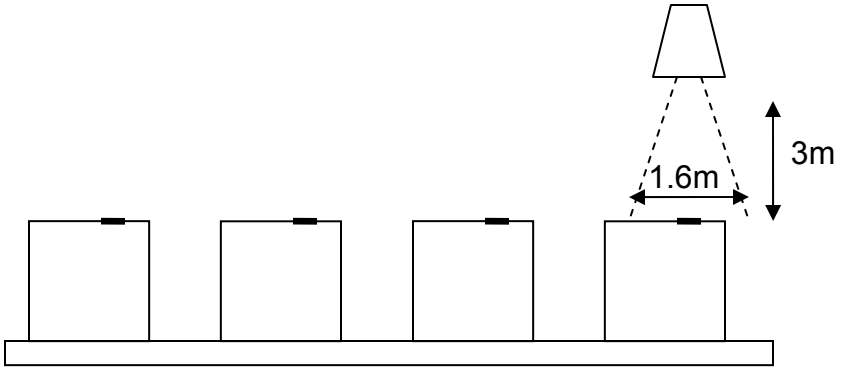


Figure 47. Minimum separation distances when range is 3 meters.

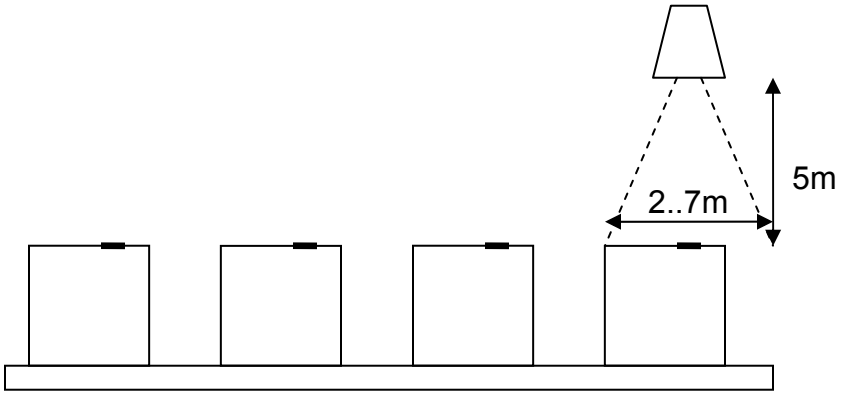


Figure 48. Minimum separation distances when range is 5 meters.

For ranges of 1 to 3 meters, the minimum separation is easily achievable since the size of each case is typically larger than the minimum separation distance required. For smaller cases, or for item level tagging where the size of the items are smaller than the minimum separation distance, a deliberate attempt has to be made to separate the items if single tag interrogation is to be ensured. As the read range increases, the separation required for single tag interrogation increases. Should this minimum not be met, tag collisions will occur and anti-collision protocols need to be effected.

From the above, we conclude that DoD's requirements can be met, and high read reliability achieved if single tag interrogation is used. At a SNR of at least 7.5 dB (see figure 37), the bit error rate is only 10^{-5}.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSIONS

The reliability of an RFID system is dependant on many factors. Some of these factors can be controlled, but many others are beyond control. Physical constraints and environmental conditions are two of the many other factors that will affect the readability of the tags.

This research has identified the factors that affect the read reliability of RFID tags, and established the relationships between the variation of each of the factors and their impacts on the read reliability. Alternative modulation/coding techniques have demonstrated an improvement in the read reliability of RFID systems. In fact, the proposed method of coding that combines repetition code with code shift keying shows a 6.5 dB improvement as compared to the coding technique used in many of today's RFID system.

B. RECOMMENDATIONS

This research has demonstrated the advantages of alternative modulation/coding techniques. Simulation runs for the proposed alternative produced results for only 2 bits per tag. Additional simulations with increased data capacity per tag can be carried out (perhaps up to the 64 or 96 bits required by US DoD).

This research has focused on the single tag problem. Future work can explore the impact of having multiple tags in the interrogation zone. For one, the proposed coding scheme will be able to detect a collision since the superposition of two or more tags will produce an invalid code word. Analysis on whether the codes provide any advantage in terms of resolving collisions can also be explored.

The model developed in this research has not taken into account the reflections by objects in the vicinity. Electromagnetic field emitted by the reader can be reflected (by metallic objects) or absorbed (by radar absorbent objects);

the reflected fields are superimposed upon the primary field emitted by the reader, and can lead to either cancellations or amplifications of the field. The effect of such reflections on read reliability can be studied.

LIST OF REFERENCES

Cha, Kainan, "Adaptive and Probabilistic Power Control Algorithms for Dense RFID Reader Network," Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Control, ICNSC '06, pp.474-479, April 2006.

Electro-com, "RFID Overview," http://www.electrocom.com.au/rfid_2.htm, last accessed May 2006.

FCC Code of Federal Regulations, Title 47, Volume 1, Part 15, Sections 245-249, February 16, 2006.

Finkenzeller, Klaus, *RFID Handbook*, John Wiley & Sons Ltd, 2003.

Gardner, Floyd and Baker, John, *Simulation Techniques: Models of Communication Signals and Processes*, John Wiley & Sons, 1997.

Glover, Bill and Bhatt, Himanshu, *RFID Essentials,* O Reilly Media Inc, 2006.

Ha, Tri T., Naval Postgraduate School EC4550 Course Notes, 2006.

Jiang, Bing, "Unobtrusive Long-Range Detection of Passive RFID Tag Motion," IEEE Transactions on Instrumentation and Measurement, Vol. 55, No. 1, pp. 187-196, February 2006.

King, Pat, "Six Sigma and the Single Tag," RFID Journal, 30 Jan 2006.

Lahiri, Sandip, *RFID Sourcebook*, IBM Press, 2006.

Lin, Shu and Costello, Daniel J., *Error Control Coding*, Pearson Prentice Hall, 2004.

Moon, Todd K., *Error Correcting Coding: Mathematical Methods and Algorithms*, John Wiley & Sons, 2005.

Nikitin, P. V. and Rao, K. V. S., "Performance Limitations of Passive UHF RFID Systems", Proceedings of IEEE Antennas and Propagation Symposium, Albuquerque, NM, pp. 1011-1014, July 2006.

Shepard, Steven, *RFID Radio Frequency Identification*, McGraw-Hill Networking, 2005.

Sklar, Bernard, *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001.

Stutzman, Warren L. & Thiele, Gary A., *Antenna Theory and Design,* John Wiley & Sons, 1997.
Tag Master, "S1255 Mark Tag Read/Only ID-Tag datasheet," http://www.tagmaster.se/downloads.php, last accessed July 2006.

US Department of Defense, Military Handbook and Standards relating to reliability, Handbook 217, http://www.weibull.com/knowledge/milhdbk.htm#200, last accessed August 2006.

US Department of Defense, Radio Frequency Identification (RFID) Policy, 30 July 2004, http://www.acq.osd.mil/log/rfid/Policy/RFID%20Policy%2007-30-2004.pdf, last accessed October 2006.

US Department of Defense, Suppliers' Passive RFID Information Guide, ver. 8.0, http://www.acq.osd.mil/log/rfid/DoD_Suppliers%27_Passive_RFID_Information_Guide_v8.0.pdf, last accessed October 2006.

Wolstenholme, Linda C., *Reliability Modelling: A Statistical Approach*, Chapman & Hall, 1999.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California